1 Einleitung

Das Sicherheitshandbuch für den Benutzer stellt die Sicherheitsfunktionen des BS2000 Betriebssystems vor und gibt Einsatzhinweise und Empfehlungen, wie der Leser Daten und Programme vor unberechtigtem Zugriff schützen kann. Der vollständige Umfang der Sicherheitsfunktionen des BS2000 steht nur dann zur Verfügung, wenn die kostenpflichtigen Software-Produkte SECOS (SEcurity COntrol System) [6], ASECO (Advanced SEcurity COntrol System) [7] und MAREN (Magnetdatenträger-Archivierungssystem im REchnerNetz) [8] installiert sind. Der Einsatz von SECOS ist Grundvoraussetzung für den sicheren Betrieb des BS2000. ASECO bietet die Funktionalität für den erweiterten Zugangsschutz mittels Chipkarte. Der Einsatz von MAREN ist Voraussetzung für den vom BS2000 gebotenen Zugriffsschutz für Magnetbänder.

Das kostenpflichtige Produkt GUARDS erweitert den Zugriffsschutz für Dateien, wie er mit FACS realisiert ist, auf einen Zugriffsschutz für Objekte. Zugriffsrechte können mit Hilfe von GUARDS und dessen Bedingungsauswertung sehr differenziert vergeben werden.

1.1 Zielsetzung und Zielgruppen des Handbuchs

Das vorliegende Sicherheitshandbuch richtet sich an den Anwender im Teilnehmerbetrieb des BS2000 V11.0. Es stellt die grundlegenden Konzepte des BS2000 zum Schutz der Vertraulichkeit und Integrität von gespeicherten Informationen dar und erläutert die Anwendung der angebotenen technischen Sicherheitseinrichtungen.

1.2 Änderungen gegenüber der Vorgängerversion

In der BS2000-Version V11.0A sind für den Benutzer folgende sicherheitsrelevante Änderungen realisiert worden:

– Einführung eines neuen Zugriffsschutzmechanismus mit Namen GUARDS. Mit GUARDS können nicht nur Dateien, sondern auch Bibliothekselemente und FITC-Ports geschützt werden.

– Privilegien können auch über Sammelprivilegien zugewiesen werden.

1.3 Konzept des Handbuchs

Die einzelnen Kapitel des Sicherheitshandbuchs behandeln weitgehend abgeschlossene Themenbereiche. Diese sollten jedoch - besonders von Benutzern ohne Vorkenntnisse - in der dargestellten Reihenfolge gelesen werden; sie können aber ebenso auch unabhängig voneinander betrachtet werden. Jedem Kapitel ist eine kurze Einführung in die behandelte Thematik vorangestellt.

Die "Einführung" gibt eine allgemeine Einführung in das Thema "Sicherheit von DV-Systemen". Es zeigt die Bedrohungen auf, denen DV-Systeme ausgesetzt sind. Weiterhin werden die Anforderungen an ein sicheres System beschrieben sowie die Maßnahmen, wie man den Bedrohungen begegnen kann.

Das Kapitel "Einführung in die Sicherheitskonzeption des BS2000" stellt die grundlegende Sicherheitskonzeption des BS2000 V11.0 vor, auf der die weiteren Kapitel des Sicherheitshandbuchs basieren.

Das Kapitel "Zugangsschutz des BS2000" beschreibt das Konzept des Zugangsschutzes und seine Anwendung.

Das Kapitel "Benutzerorganisation, Benutzerrechte und Benutzerverwaltung" beschreibt die Benutzerorganisation, die Benutzerrechte und die Benutzerverwaltung durch Gruppenverwalter.

Das Kapitel "Zugriffsschutz des BS2000" beschreibt das Konzept des Zugriffsschutzes und seine Anwendung.

Das Kapitel "Protokollierung des BS2000" beschreibt die Möglichkeiten der Protokollierung, die dem Anwender im Teilnehmerbetrieb zur Verfügung stehen.

Das Kapitel "Resümee" macht aufmerksam auf die Bedingungen, die an den Einsatz der gebotenen Sicherheitsfunktionen geknüpft sind, und faßt die Auswirkungen des sicheren Betriebs auf den Benutzer zusammen.

Anhang A stellt die sicherheitsrelevanten Kommandos des BS2000 zusammen.

Anhang B enthält eine Aufstellung der sicherheitsrelevanten Funktionseinschränkungen.

Im Kapitel "Fachwörter" werden wichtige Begriffe näher erläutert.

Der Einsatz der Sicherheitsfunktionen wird in vielen Fällen durch konkrete Beispiele verdeutlicht. Alle verwendeten Kommandos werden im SDF-Format beschrieben (Die analogen ISP-Kommandos sind dem Anhang der entsprechenden SDF-Handbücher zu entnehmen). Die Ablaufbeispiele sind so dargestellt, daß ein optimales Maß an Sicherheit gewährleistet wird. Abkürzende Schreibweisen der Kommandos sind in jedem Fall möglich, oftmals auch abkürzende Verfahren, die allerdings nicht in allen Fällen den vom BS2000 gebotenen Schutz gewährleisten.

Vorausgesetzte und weiterführende Dokumente

Für die Lektüre des Sicherheitshandbuchs wird die Kenntnis des folgenden Handbuchs vorausgesetzt:

– "BS2000-Benutzerkommandos (SDF-Format)" [9]

Weiterführende Informationen finden Sie in den Handbüchern

– "BS2000-DVS Einführung und Kommandoschnittstelle" [10],
– "BS2000-DVS Assemblerschnittstelle" [11] und
– "BS2000-MAREN Magnetdatenträger-Archivierungssystem im Rechnernetz" [8].

Für weiterführende Informationen zum Thema "Sicherheit im BS2000" wird auf das "Sicherheitshandbuch für die Systemverwaltung des BS2000" [13] sowie das Handbuch zu SECOS [6] verwiesen.

2 Einführung

In der Industrie, bei Banken, Versicherungen, Behörden und anderen Institutionen werden heute Daten in DV-Systemen gespeichert und verarbeitet, die für den Einzelnen oder für eine ganze Organisation von eminenter Wichtigkeit sind. Neben dem Funktionalitäts- und Performance-Aspekt ist dabei ein neuer Aspekt in den Vordergrund getreten: die Sicherheit von DV-Systemen.

Kennzeichnend für diese Entwicklung ist das wachsende Bedürfnis nach Vertraulichkeit der gespeicherten Informationen bei den Benutzern von DV-Systemen - sei es der langjährig erarbeitete Wissensvorsprung eines Industrieunternehmens gegenüber seinen Konkurrenten, die Daten bezüglich einer bestimmten Personengruppe bei einer Finanzbehörde oder der Kontostand eines Sparers bei einer Bank. Die Gründe für die Wichtigkeit des Themas "Sicherheit in DV-Systemen" sind vielfältig und werden durch die Bemühungen der Hardware- und Software-Hersteller in zunehmendem Maße verdeutlicht.

Ziel dieser Bemühungen ist es, die mißbräuchliche Verwendung, die Verfälschung bzw. den Verlust von vertrauenswürdigen Informationen bei ihrer Verarbeitung und Speicherung in DV-Systemen zu verhindern.
Beeinträchtigungen der Sicherheit können auf vielfältige Weise verursacht werden:

- durch menschliches Fehlverhalten, wie Drücken einer falschen Taste, Start eines falschen Programms, Verlust eines Speichermediums etc.,
- durch spielerischen Forscherdrang des Benutzers,
- durch kriminelle Aktivitäten, angefangen vom jugendlichen Hacker, der auf seine geniale Begabung durch eine originelle Meldung aufmerksam machen möchte, bis zum professionellen Spionageteam, das wirtschaftliche oder militärische Geheimnisse ausspähen will,
- durch Hardware- oder Software-Fehler, wie Funktionsstörungen der CPU, Übertragungsfehler, Programmfehler etc.,
- durch höhere Gewalt, wie Stromausfall, Feuer, Wassereinbruch, Erdbeben etc.

Der Gesetzgeber hat sich des Themas Sicherheit deshalb schon vor längerer Zeit angenommen. Bundes- und Landesdatenschutzgesetze [1], [2] sowie diverse Rechtsvorschriften regeln den Umgang mit personenbezogenen Daten. Für die Hardware- und Software-Hersteller stellt sich heute- und in der Zukunft zunehmend wichtiger- die Aufgabe, die technische Basis für die Sicherheit von DV-Systemen und damit für die Realisierung von Datenschutz zu schaffen und weiterzuentwickeln.

Technische Sicherheitseinrichtungen eines Herstellers bleiben jedoch weitgehend nutzlos, wenn sie nicht durch organisatorische Maßnahmen des Anwenders ergänzt werden. Die Verantwortung für den Datenschutz trägt allein der Anwender eines DV-Systems. Er muß, zusätzlich und eigenverantwortlich,

- die gesetzlichen Vorschriften zum Datenschutz beachten,
- die Grundsätze und Richtlinien seines Unternehmens zum Datenschutz einhalten und
- beim Umgang mit zu schützenden Daten problembewußt handeln,

um Datenschutz zu erreichen.

2.1 Allgemeine Bedrohungen für DV-Systeme

In Abhängigkeit von der Aufgabe und der Einsatzumgebung sowie der Sensitivität der gespeicherten Informationen kann man drei allgemeine Bedrohungen unterscheiden, die die Sicherheit eines DV-Systems gefährden (siehe Bild 1):

– den Verlust der Vertraulichkeit,
– den Verlust der Integrität und
– den Verlust der Verfügbarkeit.

Diese Grundbedrohungen gilt es durch geeignete Maßnahmen in der Einsatzumgebung des DV-Systems sowie innerhalb des DV-Systems selbst zu verringern und im Idealfall ganz auszuschalten.

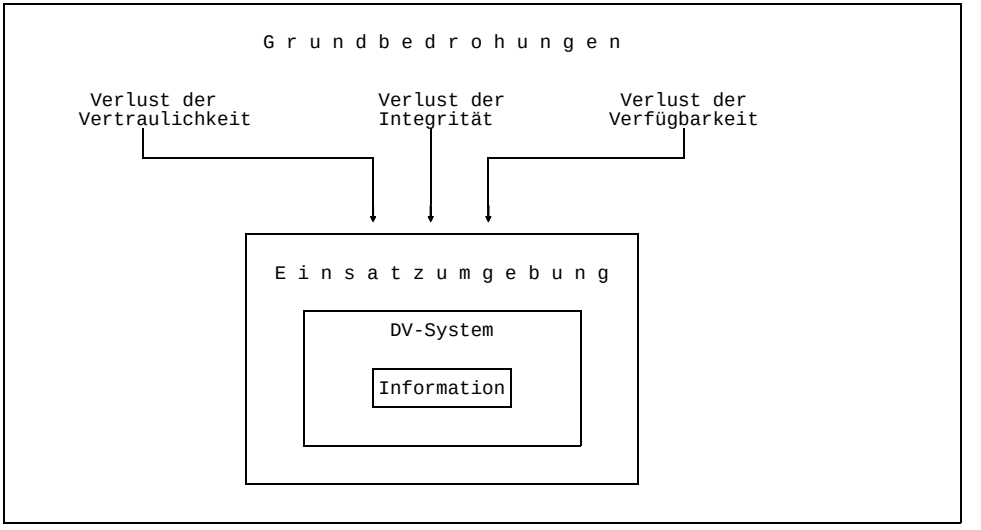


Bild 1: Grundbedrohungen für DV-Systeme

Verlust der Vertraulichkeit

Die Vertraulichkeit der in einem DV-System gespeicherten Informationen ist dann gewährleistet, wenn eine unberechtigte Kenntnisnahme und damit ein Informationsgewinn durch unbefugte Personen ausgeschlossen werden kann. Der Verlust der Vertraulichkeit ist gegeben, wenn die gespeicherten Informationen nicht mit der notwendigen Sorgfalt bezüglich ihrer Geheimhaltung behandelt werden können.

Schutzwürdige Informationen dürfen prinzipiell nur denjenigen Personen zugänglich sein, die diese Informationen für die Erfüllung ihrer Aufgaben unbedingt benötigen bzw. für den Zugriff eine besondere Autorisierung besitzen. Die Möglichkeit der unberechtigten Kenntnisnahme von Informationen kann in einem Betriebssystem z.B. durch den Einsatz wirksamer Zugangsschutz- und Zugriffsschutzmechanismen oder durch Verschlüsselung bedeutend verringert werden.

Verlust der Integrität

Die Integrität von gespeicherten Informationen setzt drei Eigenschaften voraus:

- ihre Vollständigkeit,
- ihre Unversehrtheit und
- ihre Korrektheit.

Die Vollständigkeit der Informationen bedeutet hier, daß bei jeder Verarbeitung alle benötigten Informationen vorhanden sein müssen. Die Unversehrtheit der Informationen bezeichnet ihre fehlerlose Speicherung. Unter der Korrektheit der Informationen versteht man ihre fehlerfreie Abbildung aus der realen Welt.

Der Verlust der Integrität von gespeicherten Informationen kann durch Fehler oder durch unberechtigte Modifikation der Informationen bewirkt werden. Der konsequente Einsatz von Zugangsschutz- und Zugriffsschutzmechanismen trägt dazu bei, die Integrität der gespeicherten Informationen zu sichern.

Verlust der Verfügbarkeit

Die Verfügbarkeit eines DV-Systems ist dann gegeben, wenn sämtliche gespeicherten Informationen und alle Systemfunktionen (Hardware- bzw. Software-Komponenten) zu jedem Zeitpunkt, zu dem sie benötigt werden, in ihrem vollen Umfang benutzt werden können. Der Verlust der Verfügbarkeit kann durch Fehler, aber auch durch unberechtigte Eingriffe in die Hardware- bzw. Software-Konfiguration bewirkt werden.

Ausfallsichere und fehlertolerante DV-Systeme werden z.B. in der Echtzeitverarbeitung gefordert. Eine wesentliche Verbesserung der Verfügbarkeit erreicht man z.B. durch Redundanz von Hardware-Komponenten, die im fehlerfreien Betrieb auch zur Leistungserhöhung des Systems eingesetzt werden können. Zur Erhöhung der Verfügbarkeit eines DV-Systems dient ebenfalls der Einsatz wirkungsvoller Zugangsschutz- und Zugriffsschutzmechanismen.

2.2 Allgemeine Sicherheitsanforderungen eines Betreibers

Die Sicherheitsanforderungen des Betreibers eines DV-Systems orientieren sich i. a. an den oben beschriebenen Grundbedrohungen für DV-Systeme und daneben an den spezifischen Bedrohungen seiner speziellen Systemumgebung, die durch eine Bedrohungsanalyse festgestellt werden müssen. Ziel ist die möglichst weitgehende Abwehr aller Bedrohungen entsprechend dem individuellen Sicherheitsbedarf des Betreibers.

Den Grundbedrohungen kann durch

– technische Sicherheitsanforderungen und den daraus abgeleiteten technischen Sicherheitsmaßnahmen

begegnet werden. Zur Abwehr der spezifischen Bedrohungen sind zusätzliche

– organisatorische Sicherheitsanforderungen und die daraus abgeleiteten organisatorischen, personellen und baulichen Sicherheitsmaßnahmen

notwendig. Technische Sicherheitsmaßnahmen bilden die Basis für die definierbare und prüfbare Sicherheit eines DV-Systems. Sie sind die Voraussetzung für organisatorische Sicherheitsmaßnahmen. Nur in ihrer Summe können technische und organisatorische Maßnahmen den Sicherheitsanforderungen eines Betreibers weitestgehend gerecht werden.

2.2.1 Allgemeine technische Sicherheitsanforderungen

Die technischen Anforderungen an die definierbare und prüfbare Sicherheit von DV-Systemen werden durch Bewertungskriterien festgelegt, die für die Bundesrepublik Deutschland in den IT-Sicherheitskriterien [3] niedergelegt sind. Die IT-Sicherheitskriterien beinhalten Funktionalitätsklassen von Sicherheitsfunktionen, die den Umfang der von einem DV-System gebotenen Sicherheitsfunktionen angeben. Zu jeder Funktionalitätsklasse setzen Qualitätsstufen einen Maßstab für den Grad des Vertrauens, der DV-Systemen mit den definierten Sicherheitsfunktionen entgegengebracht werden kann.

Im Rahmen der Bemühungen die vorhandenen Sicherheitskriterien zu harmonisieren, haben Deutschland, Frankreich, Großbritannien und die Niederlande gemeinsame, europäische Kriterien entwickelt, die Information Technology Security Evaluation Criteria (ITSEC) [40]. Diese sind eng an die IT-Sicherheitskriterien angelehnt und werden diese in Zukunft ersetzen.

Grundlage für die Bewertung eines DV-Systems sind die Sicherheitskriterien. Die Bewertung eines DV-Systems erfolgt unter den Gesichtspunkten Funktionalität und Qualität.

Die zu bewertende Funktionalität wird durch die Sicherheitsanforderungen festgelegt. Sie kann auch durch einen oder mehrere Funktionalitätsklassen beschrieben werden. Bei der Bewertung wird dann geprüft, ob und mit welcher Effektivität die Sicherheitsfunktionen des DV-Systems die Sicherheitsanforderungen erfüllen.

Bei der Bewertung der Qualität wird die Korrektheit der Implementierung der Sicherheitsfunktionen bewertet. Dies geschieht durch eine detaillierte Analyse der Dokumentation des DV-Systems sowie der bereitgestellten Anwenderdokumentation. Weitere Qualitätsaspekte sind die Wirksamkeit der Sicherheitsmechanismen, der Herstellungsvorgang, die Betriebsqualität und anderes mehr.

Die Sicherheit eines DV-Systems und insbesondere des ihm zugrundeliegenden Betriebssystems kann nur dann beurteilt werden, wenn nachprüfbar ist, inwieweit die Sicherheitsanforderungen vom DV-System korrekt eingehalten werden. Die Sicherheitsmechanismen werden also sowohl isoliert auf ihre Wirksamkeit geprüft als auch in ihrer Gesamtheit und ihrem Zusammenwirken hinsichtlich konkreter Sicherheitsanforderungen beurteilt, die das DV-System zu unterstützen und durchzusetzen hat.

Von entscheidendem Einfluß auf die Sicherheitsfunktionalität eines Betriebssystems ist die Mächtigkeit seines Einsatzspektrums. Universal-Betriebssysteme wie das BS2000 sind Multi-Task- und Multi-User-Systeme, die einer ständig steigenden Anzahl von Benutzern die parallele Ausführung einer immer größeren Anzahl von Aufträgen gestatten. Sie unterstützen einerseits den Teilnehmerbetrieb mit Dialog- und Stapelverarbeitung und ermöglichen andererseits im Teilhaberbetrieb den Einsatz von Transaktions- und Anwendungssystemen, wobei diese Betriebsarten sowohl unabhängig voneinander als auch kombiniert von einem Betreiber genutzt werden können.

Technische Sicherheitsmaßnahmen

Zu den wichtigsten technischen Sicherheitsmaßnahmen zählen Maßnahmen zum Zugangsschutz, zum Zugriffsschutz und zur Protokollierung. Diese sind Gegenstand des vorliegenden Sicherheitshandbuchs und werden in den folgenden Kapiteln ausführlich behandelt.

2.2.2 Allgemeine organisatorische Sicherheitsanforderungen

Für die organisatorischen Sicherheitsanforderungen und die daraus abgeleiteten Sicherheitsmaßnahmen ist der Betreiber eines DV-Systems zuständig. Der Benutzer kann sie zum Teil nur indirekt beeinflussen, gleichwohl sollte er von ihrer Existenz wissen, um im Einzelfall sein Verhalten darauf abzustimmen.

Organisatorische Schutzmaßnahmen bilden die Grundlage für die sichere Umgebung eines DV-Systems. Die Anforderungen an eine sichere Systemumgebung werden hauptsächlich von zwei Faktoren beeinflußt:

- vom Personenkreis, der das DV-System benutzt, und
- von der Infrastruktur, in die das DV-System eingebettet ist.

Die größten Bedrohungen gehen im Normalbetrieb eines DV-Systems vom Personenkreis aus, der es benutzt. Der Zutritt zur Rechenanlage wird in der Regel nur ausgewählten Personen gestattet sein. Die Benutzung des DV-Systems sollte durch Richtlinien wie z. B. eine Rechenzentrumsbenutzerordnung festgelegt sein. Die vorhandenen Sicherheitseinrichtungen müssen - soweit erforderlich - allgemein bekannt und akzeptiert sein. Alle Benutzer sollten für die Sicherheitsbelange des DV-Systems motiviert und entsprechend geschult werden. Motivation und Schulung der Benutzer kann z.B. durch ein Sicherheitsprogramm unterstützt werden, das Ziele formuliert und die Überprüfung von Fortschritten ermöglicht.

Die Sicherheitsanforderungen an die Infrastruktur eines DV-Systems betreffen bauliche Schutzmaßnahmen zum Schutz eines DV-Systems vor Gefahren durch Hitze, Feuer, Wasser, Einbruch, Diebstahl, Sabotage etc. Diese müssen durch Regelungen für das Verhalten bei Notfällen und Katastrophen unterstützt werden.

Weiterführende Hinweise findet der interessierte Leser im Fragenkatalog zu Sicherheitsvorkehrungen für Rechenzentren [4] und im Leitfaden für Katastrophenpläne [5].

Organisatorische und personelle Sicherheitsmaßnahmen

Organisatorische Sicherheitsmaßnahmen sind sehr spezifisch auf den Sicherheitsbedarf eines Betreibers ausgerichtet. Sie betreffen die Aufbau- und Ablauforganisation im DV-Bereich und lassen sich oft problemlos und kostengünstig auch in einen bereits laufenden Betrieb einfügen.

Beispiele für organisatorische und personelle Sicherheitsmaßnahmen, die in erster Linie für den Betreiber eines DV-Systems relevant sind:

- Unmißverständliche Zuordnung von Verantwortlichkeiten,
- Funktionstrennung z. B. in Maschinenbedienung, Arbeitsvorbereitung, Programmierung systemnaher Software und Anwendungsprogrammierung,
- Zutrittskontrollen zur Rechenanlage.

Beispiele für organisatorische und personelle Sicherheitsmaßnahmen, die in erster Linie für den Benutzer eines DV-Systems relevant sind:

- Überprüfung der Verarbeitung personenbezogener Daten durch den internen Datenschutzbeauftragten,
- Richtlinien und Hinweise zur Behandlung von Kennwörtern und Chipkarten,
- Regelungen zum Löschen von Daten,
- Regelungen zur Sicherung von Programmen und Daten,
- Regelungen für die Entwicklung und Freigabe von Programmen,
- Richtlinien zur Behandlung von Datenträgern,
- Richtlinien für den Umgang mit fremden Programmen.

2.3 Grundlegende Begriffe

Zum besseren Verständnis der folgenden Kapitel des Sicherheitshandbuchs werden an dieser Stelle in alphabetischer Anordnung die wichtigsten sicherheitsrelevanten Begriffe erläutert.

Datenschutz

Datenschutz bezeichnet die Menge aller Vorkehrungen zur Verhinderung unerwünschter Folgen der automatischen Datenverarbeitung für Individuen. Er sichert die schutzwürdigen Belange von Einzelpersonen durch gesetzliche Normierung des Umgangs mit personenbezogenen Daten.

Zu den Datenschutzgesetzen zählen das Bundesdatenschutzgesetz [1] und die Landesdatenschutzgesetze [2]. Es sind aber auch andere Rechtsvorschriften zu beachten, die Regelungen zum Datenschutz enthalten wie das Gesetz über das Postwesen, das Fernmeldeanlagengesetz und das Personenstandsgesetz.

Datenschutz wird realisiert durch die Einhaltung von Vorschriften, durch problembewußtes Handeln und durch die Anwendung der Datensicherung.

Datensicherheit

Datensicherheit ist das Ergebnis der Datensicherung, also der technischen und organisatorischen Maßnahmen zum Schutz der Funktionsfähigkeit eines DV-Systems und der gespeicherten Informationen gegen Mißbrauch.

Datensicherung

Der Begriff Datensicherung tritt bei der Realisierung des Datenschutzes auf und bezieht sich auf alle schutzwürdigen Daten. Er bezeichnet die Menge aller Vorkehrungen und Maßnahmen

- organisatorischer,
- baulicher,
- maschinentechnischer,
- programmtechnischer,
- verfahrenstechnischer,
- personeller und
- sonstiger Art

zum Schutz eines DV-Systems (Hardware, Programme, Daten) vor

- Störung,
- Verlust (z.B. durch Fehler, Katastrophen etc.) und
- Mißbrauch (z.B. durch unberechtigten Zugriff).

Objekt

Ein Objekt ist ein passives Element eines DV-Systems, das Informationen enthält oder aufnimmt und auf das eine Operation wie Lesen, Schreiben, Ausführen etc. angewendet werden kann. Der Zugriff auf ein Objekt impliziert im allgemeinen den Zugriff auf die Daten, die das Objekt enthält.

Beispiele für Objekte sind:

- Datenträger,
- Dateien,
- Guards,
- FITC-Ports,
- Datensätze,
- Speicherbereiche,
- Adreßräume,
- Kommunikationsverbindungen,
- Geräte.

Referenz-Monitor

Dem Konzept des Referenz-Monitors liegt ein abstraktes Modell zugrunde, nach dem in einem DV-System alle Zugriffe von Subjekten auf Objekte durch einen Mechanismus gesteuert und überwacht werden, d.h. der bei jedem Zugriffswunsch darüber entscheidet, ob das Subjekt überhaupt zugreifen darf und welche Operationen es auf dem Objekt ausführen darf. Dieser Mechanismus wird als Referenz-Monitor bezeichnet. Die Entscheidungsgrundlage für den Referenz-Monitor, bildet die Autorisierungsdatenbasis, eine interne Darstellung der Zugriffsregeln einer vorgegebenen Sicherheitspolitik. Die einzelnen Zugriffe werden vom Referenz-Monitor protokolliert und als Revisionsdaten für Revisionszwecke gespeichert.

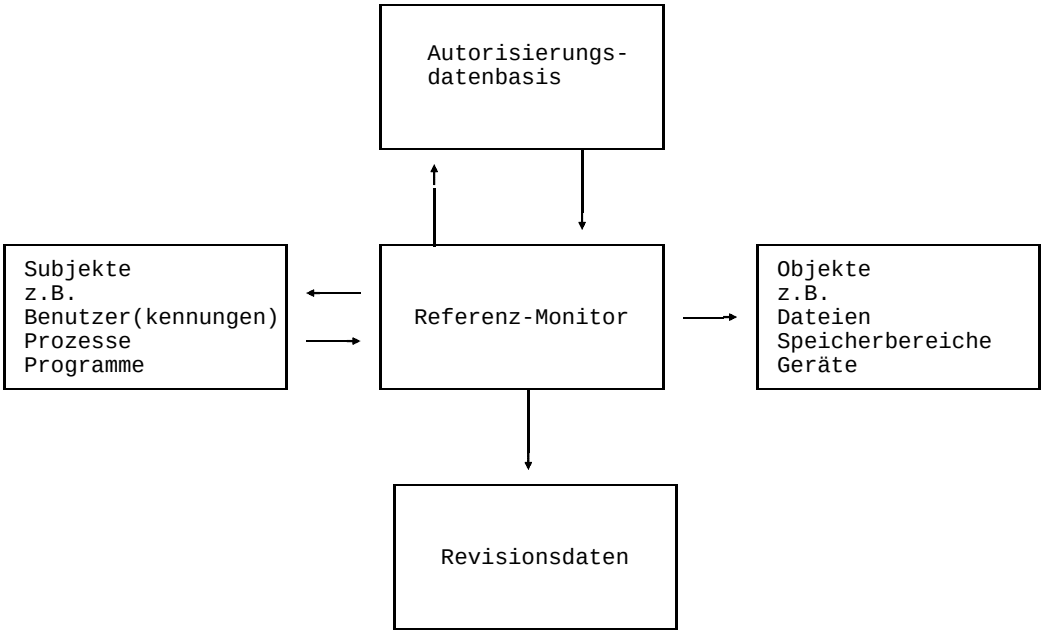


Bild 2: Mechanismus des Referenz-Monitors

An die Realisierung eines Referenz-Monitors werden drei wesentliche Entwurfsanforderungen geknüpft. Der Referenz-Monitor muß

- bei allen Zugriffen beteiligt sein,
- gegen unbefugte Eingriffe geschützt sein und
- nachweisbar korrekt arbeiten.

Die konkrete Implementierung eines Referenz-Monitors in einem Betriebssystem mit Hilfe von Hardware, Firmware und Software wird als Sicherheitskern bezeichnet. Zusätzlich zu den Funktionen, die im Sicherheitskern realisiert werden müssen, gibt es weitere Funktionen, die sicherheitsrelevant sind, z.B. Funktionen zur Identifizierung und Authentisierung. Alle Sicherheitsfunktionen können nur dann auf ihre Korrektheit überprüft werden, wenn sie in einer vom restlichen Betriebssystem abgegrenzten Komponente, der sicheren Rechenbasis (Trusted Computing Base), angesiedelt werden. Die Realisierung einer sicheren Rechenbasis in ihrer Idealform ist praktisch nur im Rahmen einer Neuentwicklung möglich. Der nachträgliche Einbau in vorhandene Betriebssysteme führt zu Einschränkungen in der Realisierung.

Sicheres DV-System

Ein DV-System wird als sicher bezeichnet, wenn das DV-System die bestehenden Bedrohungen entsprechend der an es gestellten Sicherheitsanforderungen abwehrt.

Sicherheitsanforderungen

Unter den Sicherheitsanforderungen an ein DV-System werden sämtliche Regeln, d.h. die gesetzlichen und die internen Bestimmungen, Vorschriften und Verfahren, verstanden, die festlegen, wie eine Organisation schutzbedürftige Informationen handhabt, insbesondere schützt und verteilt.

Software-Konfiguration für den sicheren Betrieb

Unter der Software-Konfiguration für den sicheren Betrieb werden sämtliche Software-Komponenten eines Herstellers verstanden, mit denen ein sicherer Betrieb gemäß dem Zertifikat der ausstellenden Behörde möglich ist. Der Einsatz der Software-Komponenten, die die evaluierten Sicherheitsfunktionen realisieren, ist dabei zwingend notwendig; alle weiteren durch das Zertifikat zugelassenen Software-Komponenten können eingesetzt werden, ohne daß dadurch das Zertifikat ungültig wird.

Subjekt

Ein Subjekt ist ein aktives Element eines DV-Systems, von dem eine Operation wie Lesen, Schreiben, Ausführen etc. ausgehen kann, die einen Informationsfluß bewirkt oder den Systemzustand ändert.

Beispiele für Subjekte sind:

- Benutzer(-kennungen),
- Datensichtstationen,
- Prozesse,
- Programme.

Die Festlegung einer Systemkomponente, Subjekt oder Objekt zu sein, sind in einem DV-System nicht statisch ein für allemal festgelegt. Subjekte können im Verlauf eines Prozesses auch als Objekte auftreten und umgekehrt. Beispielsweise kann ein Prozeß, der von einem anderen Prozeß gestartet wird, bezogen auf diese Aktion ein passives Element und damit ein Objekt sein, während er für alle Aktionen (z.B. Dateizugriffe), die von ihm selbst ausgehen, ein aktives Element, also ein Subjekt, darstellt.

Zugangsschutz

Zugangsschutz beinhaltet alle Methoden zum Schutz eines DV-Systems vor unberechtigtem Systemzugang. Ziel der Methoden ist die eindeutige Identifizierung und Authentisierung der Benutzer, ohne die ein wirksamer Zugriffsschutz für die Objekte des DV-Systems nicht gewährleistet werden kann. Die heute gängigen Verfahren zum Zugangsschutz beruhen meistens auf Kennwörtern. Deutlich höheren Zugangsschutz erreicht man durch den Einsatz der Chipkarte. Verfahren zur Überprüfung von biometrischen Merkmalen, wie Fingerabdruck oder Retina, für den Zugangsschutz befinden sich derzeit noch in der Entwicklung.

Zugriffsschutz

Zugriffsschutz bezeichnet die Regeln, nach denen in einem DV-System Subjekte auf Objekte zugreifen können, und die Methoden, mit denen die Einhaltung dieser Regeln sichergestellt werden kann. Unter Zugriff werden dabei Operationen wie Lesen, Schreiben, Ausführen etc. von Programmen oder Daten verstanden. Eine Möglichkeit, die Zugriffsrechte der Subjekte intern zu speichern, sind Zugriffskontrollisten (Access Control Lists).

Ein Zugriffsschutz kann auch über Zugriffsbedingungen erreicht werden. GUARDS stellt eine Bedingungsauswertung für Objektverwaltungen zur Verfügung. Eine Objektverwaltung (dies können DVS, LMS, FITC oder eigene Programme sein) stellt die Anfrage an GUARDS, ob die Zugriffsbedingungen, die in einem Guard hinterlegt wurden, zum Zeitpunkt der Anfrage erfüllt sind. GUARDS wertet die im angegebenen Guard abgelegten Bedingungen aus und übermittelt das Ergebnis "Bedingung erfüllt" oder "Bedingung nicht erfüllt" an die Objektverwaltung. Diese verwendet das Ergebnis der Auswertung, um einen Zugriff zu gestatten oder nicht.

3 Einführung in die Sicherheitskonzeption des BS2000

Das BS2000 ist ein Universal-Betriebssystem, das durch seine Betriebsarten den Teilnehmerbetrieb ebenso wie den Teilhaberbetrieb unterstützt. Seine Sicherheitsfunktionen gewährleisten, daß eine Vielzahl von Benutzern die gebotenen Systemdienstleistungen unabhängig voneinander nutzen kann, ohne sich gegenseitig zu stören - sei es zufällig oder absichtlich. Die Sicherheitsfunktionen sind im Kern des BS2000 und den zugehörigen Subsystemen verankert.

Das vorliegende Sicherheitshandbuch beschränkt sich auf den Teilnehmerbetrieb des BS2000 V11.0. Das Kapitel beschreibt die grundlegenden Aufgabenbereiche, die im Teilnehmerbetrieb des BS2000 unterschieden werden können, und stellt auf diesem Hintergrund die Grundsätze vor, auf denen die Sicherheitskonzeption des Betriebssystems basiert.

3.1 Grundlegende Aufgabenbereiche im BS2000

Das BS2000 unterscheidet im Teilnehmerbetrieb drei verschiedene Arten von Systembenutzern:

- die Anwender im Teilnehmerbetrieb,
- die Systemverwaltung und
- die Systembedienung.

Den verschiedenen Arten von Systembenutzern lassen sich unterschiedliche Aufgabenbereiche zuordnen. Jeder Aufgabenbereich ist mit bestimmten Funktionen und Rechten ausgestattet. Anwender im Teilnehmerbetrieb sind im Regelfall die überwiegende Mehrzahl der Systembenutzer. Die Systemverwaltung und Systembedienung ist dagegen einer kleinen Anzahl besonders autorisierter Personen vorbehalten. Im BS2000 sind Aufgaben an Kennungen und eventuell besondere Terminals (Konsole) gekoppelt. Diesen Kennungen werden Privilegien und die damit verbundenen Aufgaben zugeordnet. Hat ein Benutzer Zugang zu einer Kennung, so kann er die Aufgaben, die mit dieser Kennung verbunden sind, wahrnehmen. Deshalb können die Aufgaben eines Aufgabenbereichs von mehreren Personen ausgeführt werden (mehrere Personen haben Zugang zu einer Kennung); eine Person kann aber ebenso in mehreren Aufgabenbereichen tätig sein (eine Person hat Zugang zu mehreren Kennungen).

Ein Betreiber des BS2000 hat die Möglichkeit, die Aufteilung der Benutzerwelt entsprechend seines individuellen Sicherheitsbedarfs vorzunehmen.

Anwender im Teilnehmerbetrieb

Der Anwender im Teilnehmerbetrieb des BS2000 kann die Betriebsarten Dialog- und Stapelbetrieb nutzen. Ihm stehen als nicht-privilegierter Systembenutzer über Kommandos, Makros und Dienstprogramme bestimmte Dienstleistungen des Betriebssystems zur Verfügung. Diese umfassen im allgemeinen:

- das Erzeugen, Starten und Steuern von Programmen,
- das Erzeugen, Starten und Steuern von Kommandoprozeduren,
- das Anfordern von Betriebsmitteln und
- den Aufruf spezieller Betriebssystem-Funktionen.

Für die Ausführung dieser Tätigkeiten bietet das BS2000 eine einheitliche Kommando- und Anweisungsoberfläche sowie eine Programmieroberfläche an (siehe "BS2000 - Technische Beschreibung - Systemübersicht" [14]).

Aufgabenbereich der Systemverwaltung

Die Systemverwaltung des BS2000 umfaßt die Planung und Steuerung des Systembetriebs gemäß strategischer Vorgaben des Betreibers. Die Systemverwaltung ist zuständig für privilegierte Verwaltungsaufgaben, um einen ordnungsgemäßen Systembetrieb des BS2000 zu gewährleisten und bei Störfällen geeignete Maßnahmen ergreifen zu können. Eine Sonderstellung innerhalb der Systemverwaltung nimmt der Sicherheitsbeauftragte ein. Ihm obliegt die Verwaltung der Systemverwalterrechte.
An die Systemverwaltung sind im allgemeinen folgende Aufgaben geknüpft:

- die Bereitstellung des Systems,
- die Auftragsabwicklung und Performance-Überwachung,
- die Verwaltung aller Benutzerkennungen und Benutzergruppen,
- die SPOOL-Verwaltung,
- die Sicherung der Datenbestände der Benutzer,
- die Vergabe und der Entzug von Systemverwalter-Rechten (Privilegien),
- die Änderung der Software-Konfiguration,
- die Anpassung der Software an geänderte Hardware-Konfigurationen,
- die Auswertung von Abrechnungsdaten, Betriebsdaten, Protokollen und Systemfehlerunterlagen und
- die Hardware- und Software-Wartung.

Zur Ausführung dieser Aufgaben stehen der Systemverwaltung eine ihren Privilegien entsprechende Ausprägung der Kommando- und Anweisungsoberfläche sowie Programmschnittstellen zur Verfügung, mit denen jederzeit in den laufenden Systembetrieb eingegriffen werden kann und die den Zugriff auf alle Dateien, Tabellen und Programme des Systems und aller Benutzer gestatten.

Aus der Menge der Systemverwalterrechte können von der Systemverwaltung bestimmte Privilegien herausgelöst und einzelnen Anwendern im Teilnehmerbetrieb zugeteilt werden. Der Aufgabenbereich der Systemverwaltung kann sich infolgedessen mit dem Aufgabenbereich des Anwenders im Teilnehmerbetrieb überschneiden. Ein (klassisches) Beispiel hierfür ist die Benutzerverwaltung. Sie ist zuständig für die hierarchische Strukturierung der Systembenutzer durch Benutzergruppen und die Verwaltung der Benutzergruppenstruktur. Zum Aufgabenbereich der Benutzerverwaltung gehören:

- das Einrichten und Löschen von Benutzerkennungen,
- die Ausstattung von Benutzerkennungen mit Benutzerrechten und Betriebsmittel-Kontingenten für die Benutzung von Betriebsmitteln,
- die Verwaltung von Benutzergruppen.

Die Grundlage für die Verwaltung der Benutzer bilden eine Berechtigung zur Ausführung bestimmter Kommandos und ein Potential an Benutzerrechten sowie Benutzerbeschreibungsdaten.

Aufgabenbereich der Systembedienung

Die Systembedienung des BS2000 ist zuständig für die Steuerung und Überwachung des laufenden Systembetriebs und der Peripherie gemäß den Vorgaben der Systemverwaltung.

Die Systembedienung hat folgende Aufgaben:

- die Inbetriebnahme des Systems,
- die Betreuung und Steuerung des laufenden Betriebs und
- die manuelle Unterstützung des Betriebs.

Der Systembedienung stehen direkt mit der Zentraleinheit verbundene Bedienplätze - die Konsolen - zur Verfügung. Für die Erfüllung ihrer Aufgaben verfügt die Systembedienung über einen speziellen Kommandosatz, mit dem sie für ihren Aufgabenbereich privilegierte Funktionen ausführen kann. Bei standardmäßiger Systemgenerierung kann die Systembedienung jedoch keine Funktionen des Anwenders im Teilnehmerbetrieb oder der Systemverwaltung ausführen.

3.2 Sicherheitsgrundsätze des BS2000

Die Sicherheitsgrundsätze des BS2000 legen fest, wie das Betriebssystem schutzbedürftige Informationen verwaltet und welche Möglichkeiten ein Betreiber des BS2000 hat, die Nutzung durch Personen zu steuern, zu regeln und zu überwachen.

Separierung

Das BS2000 bildet mit den privilegiert ablaufenden Subsystemen eine vertrauenswürdige Rechenbasis für alle Zugriffe durch Prozesse des Benutzers auf die vom BS2000 geschützten Objekte. Der Schutz der Speicherbereiche ist nach dem Schloß-Schlüssel-Prinzip realisiert durch ein Speicherschloß, das jeder Seite im Hauptspeicher zugeordnet ist, und einen vom Betriebssystem eingestellten Ablaufschlüssel.

Der Aufruf einer Systemdienstleistung durch Programmläufe des Benutzers kann nur über eine spezielle Schnittstelle (Supervisor Call) erfolgen, so daß alle Parameter auf ihre Gültigkeit überprüft werden können.
Verschiedene Benutzeraufträge werden getrennten Adreßräumen zugeordnet. Eine wechselseitige Beeinflussung ist nur über Objekte möglich, die von den beteiligten Partnern gezielt zum Zweck der Kommunikation vereinbart wurden.

Fehlerüberbrückung

Wichtige Hardware-Komponenten (Register, Busse, Verarbeitungswerke, Firmware-Speicher etc.) sind paritätsgesichert. Für defekte Spuren auf Plattenspeichern sind Ersatzspuren vorgesehen, die automatisch zugewiesen werden. Über sporadisch auftretende Fehler werden Fehlerstatistiken geführt. Bei regelmäßiger Auswertung dieser Fehlerstatistiken und Wartung der Hardware können Hardware-Fehler rechtzeitig erkannt und daraus resultierende Systemausfälle vermieden werden.
Fehler, die die Software erkennt, und solche, die die Hardware erkennt, aber nicht automatisch überbrücken kann, werden von Software-Funktionen behandelt. Zusätzlich werden zu jedem Systemfehler, auch solchen, die zu einem Systemabbruch führen, ausreichende Diagnoseinformationen hinterlegt.

Gewährleistung der Funktionalität

Das korrekte Verhalten der wichtigsten Systemkomponenten wird einerseits durch die systeminterne Fehlerüberbrückung, andererseits durch die Systembedienung erreicht. Die Systembedienung wird durch Überwachungsinformationen, die laufend an der Konsole ausgegeben werden, auf bereits bestehende oder sich anbahnende Fehlersituationen hingewiesen. Sie kann von sich aus die Hardware-Konfiguration des Systems verändern, insbesondere Hardware-Komponenten zu- und wegschalten. Die Funktionalität wird zusätzlich durch systeminterne Regelmechanismen gewährleistet, die auf Ausnahmesituationen automatisch reagieren.

3.2.1 Sicherheitsgrundsätze für den Benutzer

Zugangsschutz (Identifizierung, Authentisierung)

Natürliche Personen benötigen eine Benutzerkennung, um Zugang zum BS2000 zu erhalten und mit dem Betriebssystem arbeiten zu können:

- Eine Person kann mehrere verschiedene Benutzerkennungen besitzen. Sie wird dann vom BS2000 aber so bedient, als würde es sich um getrennte Personen handeln.
- Mehrere Personen können gemeinsam eine Benutzerkennung besitzen. Sie werden dann aber bezüglich der Abwicklung ihrer Tätigkeiten vom BS2000 nicht voneinander unterschieden. Nur im Rahmen der Beweissicherung wird beim Einsatz der Chipkarte [7] eine personenbezogene Unterscheidung getroffen.

Die rechtmäßige Verwendung einer Benutzerkennung wird bei jedem Systemzugang durch ein Identifizierungs- und Authentisierungsverfahren überprüft. Dabei wird nach erfolgter Identifizierung eine Verifikation der Identität z.B. durch Kennwort- und/oder Chipkartenverfahren durchgeführt.

Das BS2000 unterscheidet fünf Zugangsklassen:

- DIALOG,
- BATCH
- REMOTE BATCH
- OPERATOR-ACCESS-TERMINAL
- OPERATOR-ACCESS-PROGRAM

Jede Zugangsklasse kann durch ein Kennwortverfahren geschützt werden, die Zugangsklassen DIALOG und OPERATOR-ACCESS-TERMINAL können zusätzlich durch ein Chipkartenverfahren geschützt werden. Durch getrenntes Sperren einzelner Zugangsklassen kann der Systemzugang für eine Benutzerkennung weiter eingeschränkt werden.

Die Möglichkeiten der Operator-Authentisierung sind detailliert im "Sicherheitshandbuch für die Systemverwaltung" [13] beschrieben.

Die Kennwörter zur Authentisierung können über eine Generierungsoption einwegverschlüsselt im System gespeichert werden.

Fehlversuche bei der Kennworteingabe können mit Zeitstrafen oder Verbindungsabbau belegt werden.

Zugriffsschutz (Rechteverwaltung, Rechteprüfung)

Der Zugriffsschutz für ein Objekt wird durch den Eigentümer des Objekts bestimmt. Eigentümer ist immer eine Benutzerkennung. Nur die unter dieser Benutzerkennung erzeugten Aufträge können die Zugriffsrechte auf das Objekt für Benutzerkennungen festlegen und ändern.

Objekte, die der Zugriffskontrolle unterliegen, sind:

- Dateien (gemeinschaftliche Plattendateien, Dateien auf privaten Datenträgern, Dateigenerationen),
- Job-Variable,
- Datenträger (private Plattenspeicher, Magnetbänder, Magnetbandkassetten, Disketten),
- Memory-Pools,
- FITC-Ports,
- Bibliothekselemente,
- User Serialization Items und
- User Event Items.

Zugriffe auf Dateien, Bibliothekselemente und FITC-Ports werden bis auf die Ebene einzelner Benutzer kontrolliert. Zugriffsrechte werden je nach Art des Objekts durch Zugriffskontrollisten, Kennwörter oder andere Zugriffsschutzmechanismen festgelegt. Die Zugriffsrechte werden je nach Art des Objekts beim Zugriff kontrolliert.

Auftragsbeschreibungen für Stapel- oder Ausgabeaufträge sowie gestartete Stapel- oder Ausgabeaufträge sind einer Benutzerkennung zugeordnet. Sie können von Aufträgen dieser Benutzerkennung und ggf. von der Systembedienung geändert oder beeinflußt werden.

Das Eigentümerrecht einer Benutzerkennung an Objekten, Auftragsbeschreibungen und gestarteten Aufträgen kann von einer Benutzerkennung der Systemverwaltung additiv wahrgenommen werden.

Beweissicherung

Neben Systemprotokollen werden benutzerkennungsbezogene Protokolle angelegt:

- Benutzerprotokolle des Auftragsablaufs im Dialogbetrieb umfassen alle Ein- und Ausgaben an einer Datensichtstation. Benutzerprotokolle des Auftragsablaufs im Stapelbetrieb enthalten alle Kommandos und die durch sie bewirkten Ereignisse, wobei Kennwortangaben durch Pseudozeichen ersetzt werden.
- Die Protokollierung von Daten zur Benutzer- und Betriebsabrechnung kann vom Benutzer durch eigene Abrechnungssätze ergänzt werden.
- Die Protokollierung sicherheitsrelevanter Ereignisse zu Revisionszwecken wird vom Sicherheitsbeauftragten festgelegt. Der Benutzer kann bei entsprechender Berechtigung die Protokollierung von Zugriffen auf Objekte, deren Eigentümer er ist, selbst steuern.

Benutzer mit besonderen Berechtigungen können angehalten sein, die Protokollierung ihrer Aktionen einzuschalten, um Systemprotokolle zu ergänzen.

Wiederaufbereitung von Speicherobjekten

Speicherobjekte sind Objekte, deren Information in einem Speicherbereich abgelegt sind. BS2000 sorgt dafür, daß bei Zuordnung von Objekten zu einem neuen Benutzer kein Zugriff auf den früheren Inhalt möglich ist. Diese Mechanismen zur Wiederaufbereitung verhindern den Informationsfluß zwischen je zwei Nutzungen desselben Speicherobjekts durch unterschiedliche Benutzer. Dies geschieht durch Löschen des früheren Inhalts.

Objekte, die der Wiederaufbereitung des BS2000 unterliegen sind:

- Dateien,
- Job-Variablen,
- Speicherseiten des Adreßraums,
- Memory-Pools,
- Magnetbänder und Magnetbandkassetten,
- User Serialization Items und
- User Event Items.

Das Löschen der Inhalte wird je nach Art des Objekts durch ein automatisches, systemgesteuertes, benutzergesteuertes oder durch ein organisatorisches Verfahren durchgeführt.

Beweissicherung

Neben Systemprotokollen werden personenbezogene Benutzerprotokolle angelegt:

- Benutzerprotokolle des Auftragsablaufs im Dialogbetrieb umfassen alle Ein- und Ausgaben an einer Datensichtstation. Benutzerprotokolle des Auftragsablaufs im Stapelbetrieb enthalten alle Kommandos und die durch sie bewirkten Ereignisse, wobei Kennwortangaben durch Pseudozeichen ersetzt werden.
- Die Protokollierung von Daten zur Benutzer- und Betriebsabrechnung kann vom Benutzer durch eigene Abrechnungssätze ergänzt werden.
- Die Protokollierung sicherheitsrelevanter Ereignisse zu Revisionszwecken wird vom Sicherheitsbeauftragten festgelegt. Der Benutzer kann bei entsprechender Berechtigung die Protokollierung von Zugriffen auf Objekte, deren Eigentümer er ist, selbst steuern.

Benutzer mit besonderen Berechtigungen können aufgrund organisatorischer Verfahren angehalten sein, die Protokollierung ihrer Aktionen einzuschalten, um Systemprotokolle zu ergänzen.

3.2.2 Sicherheitsgrundsätze für den Betreiber

Voraussetzungen für den sicheren Betrieb des BS2000 sind die Installierung des unverfälschten Systemcodes, seine korrekte Parametrisierung und sein Arbeiten über zuverlässig erstellte Steuerdateien. Ein Betreiber des BS2000 muß diese Voraussetzungen sicherstellen. Diese sind im Sicherheitshandbuch für die Systemverwaltung des BS2000 [12] beschrieben.

Auslieferung und Installation

Der Systemcode des BS2000 kann vollständig generiert vom Hersteller übernommen oder vom Betreiber aus Komponenten des Herstellers generiert werden. Nur im ersten Fall liegt die Verantwortlichkeit für die Unverfälschtheit des Systemcodes beim Hersteller. Im zweiten Fall muß zusätzlich die unverfälschte Generierung des Betriebssystems überprüft werden.

Ein generiertes BS2000 kann bezüglich der Generierungsoptionen einem Plausibilitätstest unterzogen werden.

Die nachträgliche Änderung der Software-Konfiguration ist auf besonders ausgewählte Subsysteme beschränkt.

Betrieb und Bedienung

Ein unverfälschtes BS2000 bietet die Sicherheitsfunktionen, auf deren Grundlage der Betreiber einen sicheren Betrieb organisieren kann.

Alle Tätigkeiten, die der Steuerung und Überwachung des Betriebs dienen, werden - von den Aktivitäten des Anwenders im Teilnehmerbetrieb technisch und organisatorisch getrennt - von der Systemverwaltung und der Systembedienung wahrgenommen.

Die Systemverwaltung erfolgt über Benutzerkennungen, die mit Privilegien ausgestattet sind.

Sämtliche Aktivitäten der Systemverwaltung und Systembedienung werden aufgezeichnet.

Alle für die Benutzer- und Betriebsabrechnung relevanten Daten werden protokolliert.

Diagnose und Wartung

Diagnosedaten werden unter speziellen Benutzerkennungen der Systemverwaltung abgelegt. Schutzwürdige Adreßraum-Seiten können von ihrer Weitergabe in Diagnoseunterlagen ausgeschlossen werden.

Der Zugriff auf Prüfdaten, die für Wartungszwecke relevant sind, kann einem Wartungstechniker vom Betreiber des BS2000 über eine ausgezeichnete Benutzerkennung erlaubt werden.

4 Zugangsschutz des BS2000

Um Zugang zum BS2000 zu erhalten, muß sich der Benutzer einem Zugangskontrollverfahren unterziehen. Diese Zugangskontrolle wird zu seiner Identifizierung und Authentisierung durchgeführt. Zur Identifizierung fordert das Betriebssystem die Eingabe einer Benutzerkennung. Bei entsprechender Vorgabe durch die Benutzerverwaltung kann zusätzlich das Einstecken einer Chipkarte in ein Chipkartenterminal notwendig sein. Die Authentisierung dient zur Überprüfung, ob der Benutzer berechtigt ist, unter der eingegebenen Benutzerkennung zu arbeiten. Die Zugangskontrolle fordert dazu die Eingabe eines Kennworts. Beim Chipkartenzugang wird die Eingabe einer Persönlichen Identifikationsnummer (PIN) verlangt.

Das vorliegende Kapitel gibt zunächst einen Überblick über die grundlegenden Konzepte des Zugangsschutzes des BS2000 und informiert anschließend über die prinzipiellen Abläufe bei der Nutzung der angebotenen Zugangsschutzmechanismen. Beispiele für den Zugang zum BS2000 sowie Richtlinien und Hinweise zu organisatorischen Maßnahmen, die den Zugangsschutz des Betriebssystems wirkungsvoll ergänzen, sind am Ende des Kapitels zusammengestellt.

4.1 Benutzerkennungen und Zugangsklassen

Benutzerkennungen

Die Benutzerkennung stellt für die Verarbeitung von Aufträgen das zentrale Subjekt im BS2000 dar. Charakteristische Merkmale einer Benutzerkennung sind (siehe Seite 55):

- Benutzerbeschreibungsdaten (Name der Benutzergruppe, Versandanschrift für Ausgabelisten etc.),
- Zugangskontrolldaten, die den Zugangsschutz für die Benutzerkennung festlegen (Zugangskontrolle durch das Kennwortverfahren, Zugangskontrolle durch das Chipkartenverfahren etc.),
- Systemverwalterrechte, die ein Benutzer für die Erledigung von Aufgaben der Systemverwaltung benötigt,
- Benutzerrechte, die nicht Systemverwalterrechte sind, wie
- das Gruppenverwalterrecht,

- Benutzerrechte bezüglich einer Abrechnungsnummer (zur Verfügung stehende CPU-Zeit, Anzahl der Abrechnungssätze etc.),
- pubset-spezifische Benutzerrechte (zur Verfügung stehender Speicherplatz etc.),
- ein verfügbarer Kommandosatz, der die unter der Benutzerkennung ausführbaren Kommandos definiert,
- sonstige Benutzerrechte (Benutzung des FILE-AUDIT, privilegierte Magnetband-Verarbeitung etc.).

Das Eigentümerrecht bezüglich der ihr zugeordneten Dateien und Jobvariablen ist ebenfalls an die Benutzerkennung geknüpft. Es umfaßt das Erzeugen und Löschen dieser Objekte, sowie das Festsetzen der Attribute der Objekte z.B. der Zugriffsrechte für andere Benutzer.

Unter einer Benutzerkennung können Aufträge an das BS2000 gestellt werden. Mit Beginn der Bearbeitung wird jedem Benutzerauftrag eine Task zugeordnet, die die Privilegien der Benutzerkennung übernimmt.

Zugangsklassen

Das BS2000 bietet jedem Benutzer die Möglichkeit den Zugang zu einer Benutzerkennung in verschiedenen Zugangsklassen zu erlangen. Im Teilnehmerbetrieb unterscheidet das BS2000 fünf Zugangsklassen:

1) Zugangsklasse DIALOG

   Die Zugangsklasse DIALOG bezeichnet den Zugang zu Benutzerkennungen, die von Partnern im Netz, insbesondere von Datensichtstationen aus, durchgeführt werden können. Das Subjekt (Benutzer) befindet sich im allgemeinen außerhalb des DV-Systems. Die Information zur Identifizierung und Authentisierung muß von außen geliefert werden.

2) Zugangsklasse BATCH

   Die Zugangsklasse BATCH bezeichnet den Zugang zu Benutzerkennungen für Stapelaufträge. Das Subjekt, das einen Stapelauftrag erteilt, ist eine Task, die unter der gleichen oder einer anderen Benutzerkennung desselben Rechners abläuft. Für diese Benutzerkennung muß die Zugangskontrolle deshalb bereits erfolgreich vorausgegangen sein.

3) Zugangsklasse REMOTE BATCH

   Die Zugangsklasse REMOTE BATCH bezeichnet den Zugang zu Benutzerkennungen von einer Fernstapelstation. Das Subjekt ist ein Benutzer an einer Fernstapelstation, der sich durch eine Benutzerkennung und eine Abrechnungsnummer als berechtigt ausgewiesen hat.

4) Zugangsklasse OPERATOR-ACCESS-TERMINAL

   Die Zugangsklasse OPERATOR-ACCESS-TERMINAL bezeichnet den Zugang eines Operators von einer Datensichtstation zur Anwendung $CONSOLE. Das Subjekt (der Operator) befindet sich außerhalb des DV-Systems. Die Information zur Identifikation und Authentisierung muß von außen geliefert werden.

5) Zugangsklasse OPERATOR-ACCESS-PROGRAM

   Die Zugangsklasse OPERATOR-ACCESS-PROGRAM bezeichnet den Zugang eines programmierten Operators (OMNIS-PROP) zur Anwendung $CONSOLE. Für die Benutzerkennung, unter der der programmierte Operator gestartet wurde, muß die Zugangskontrolle bereits erfolgreich vorausgegangen sein.

Anmerkung:

Im sicheren Betrieb ist die Zugangsklasse REMOTE BATCH nicht erlaubt.

4.2 Zugangsschutzmechanismen

4.2.1 Identifizierungs- und Authentisierungsmechanismen

Die Identifizierung und Authentisierung eines Benutzers kann im BS2000 durch ein Kennwortverfahren erfolgen. Erweiterten Zugangsschutz bietet die Zugangskontrolle mittels Kennwort und Chipkarte.

4.2.2 Zugangskontrolle mittels Kennwort

Das Kennwortverfahren ist ein gedächtnisgestütztes Zugangskontrollverfahren, das auf der Kenntnis einer im Betriebssystem gespeicherten Information basiert. Nach der Eingabe einer Benutzerkennung verlangt das BS2000 vom Benutzer die Eingabe eines zugehörigen Kennworts, um ihn als berechtigten Benutzer zu akzeptieren. Der Systemzugang wird nur dann gewährt, wenn das vorgelegte Kennwort und das gespeicherte Kennwort übereinstimmen.

Zur Ergänzung des Kennwortschutzes bietet das BS2000 folgende Mechanismen an:

- die Kennwort-Verschlüsselung,
- die Festlegung der minimalen Länge eines Kennworts,
- die Festlegung der minimalen Komplexität eines Kennworts und
- die Begrenzung der Lebensdauer eines Kennworts.

Die Schutzattribute werden für existierende Benutzerkennungen durch das SET-LOGON-PROTECTION- bzw. MODIFY-LOGON-PROTECTION-Kommando (siehe Anhang A) durch die Benutzerverwaltung vereinbart. Berechtigt zur Ausführung der Kommandos sind:

- systemglobale Benutzerverwalter (d.h. Inhaber des Privilegs USER-ADMINISTRATION, siehe Seite 57ff) für alle Benutzerkennungen und
- Gruppenverwalter (siehe Seite 77 und Seite 79), die das Gruppenverwalterrecht in der Ausprägung MANAGE-MEMBERS oder MANAGE-GROUPS besitzen, für die ihrer Benutzergruppe zu- und untergeordneten Benutzerkennungen.

Kennwort-Verschlüsselung

Gesteuert über eine Generierungsoption und durch die Angabe des Operanden ENCRYPTION=YES in einem der Kommandos ADD-USER, MODIFY-USER, SET-LOGON-PROTECTION bzw. MODIFY-LOGON-PROTECTION (siehe Anhang A), können Kennwörter einweg-verschlüsselt im Betriebssystem gespeichert werden. Die Einwegverschlüsselung garantiert, daß die verschlüsselten Kennwörter mit vertretbarem Aufwand nicht mehr in ihre ursprüngliche Form überführbar sind.

Damit die Einwegverschlüsselung wirksam wird, muß sie von der Systemverwaltung bei der Systemgenerierung eingeschaltet worden sein. Danach ist sie für das gesamte System gültig.

Minimale Länge eines Kennworts

Für jedes Kennwort kann von der Benutzerverwaltung eine minimale Länge vereinbart werden.

Die Überprüfung der minimalen Länge erfolgt bei jedem Wechsel eines Kennworts durch das MODIFY-USER-PROTECTION-Kommando (siehe Anhang A). Bei der Überprüfung werden abschließende Leerzeichen als nicht signifikant betrachtet und abgeschnitten.

Minimale Komplexität eines Kennworts

Für jedes Kennwort kann von der Benutzerverwaltung eine minimale Komplexität festgelegt werden. Dabei werden vier Stufen der Komplexität unterschieden:

Stufe 1: Keine Einschränkung.

Stufe 2: Kennwort darf nur maximal zwei aufeinander folgende Zeichen enthalten, die gleich sind.

Stufe 3: Kennwort muß zusätzlich mindestens einen Buchstaben und eine Ziffer enthalten.

Stufe 4: Kennwort muß zusätzlich mindestens ein Sonderzeichen enthalten.

Die Überprüfung der minimalen Komplexität erfolgt bei jedem Wechsel eines Kennworts durch das MODIFY-USER-PROTECTION-Kommando (siehe Anhang A).

Begrenzung der Lebensdauer eines Kennworts

Die Lebensdauer eines Kennworts kann von der Benutzerverwaltung auf einen maximalen Zeitraum begrenzt werden, um den Benutzer zu zwingen, sein Kennwort in vorgegebenen Zeitabständen zu wechseln.

Die Überprüfung der Lebensdauer erfolgt für die Zugangsklasse DIALOG nach der Eingabe des LOGON-Kommandos, für die Zugangsklasse BATCH bei der Bearbeitung des ENTER-Kommandos bzw. des ENTER-Makros und für die Zugangsklasse REMOTE BATCH bei der Bearbeitung der LOGON-Karte. Falls die Lebensdauer eines Kennworts abgelaufen ist, wird die betreffende Benutzerkennung gesperrt und kann nur durch die Vergabe eines neuen Kennworts durch die Benutzerverwaltung wieder aktiviert werden. Erfolgt eine Überprüfung des Kennworts im Zeitraum von einem Monat vor Ablauf der Lebensdauer, so wird dem Benutzer bei erfolgreicher Eingabe des LOGON-Kommandos eine Warnung ausgegeben.

4.2.3 Zugangskontrolle mittels Chipkarte

Neben dem Kennwortverfahren ist das Chipkartenverfahren im BS2000 als zusätzliches Zugangskontrollverfahren für die Zugangsklassen DIALOG und OPERATOR-ACCESS-TERMINAL vorgesehen. Die Benutzerverwaltung legt fest, ob eine Benutzerkennung durch das Chipkartenverfahren geschützt wird und welche Chipkarten für die Benutzerkennung zulässig sind. Vom Benutzer kann neben der Vorlage einer gültigen Chipkarte die Kenntnis einer darin gespeicherten Autorisierungsinformation, der Persönlichen Identifikationsnummer (PIN), verlangt werden.

Die Vorteile des Einsatzes der Chipkarte sind:

- erheblicher Sicherheitsgewinn durch doppelte Sicherung (Besitz der Chipkarte und Kenntnis der PIN),
- einfache Handhabung,
- Bemerken von Verlust bzw. Diebstahl (spätestens bei der Eingabe des nächsten LOGON-Kommandos).

Systemkonfiguration für den Einsatz der Chipkarte

Für den Einsatz der Chipkarte ist folgende Hardware-Systemkonfiguration (siehe Bild 3) notwendig:

- Chipkarte,
- Chipkartenterminal (CKT) bzw. Chipkartenleser (CKL),
- Datensichtstation,
- BS2000-Rechner und
- Zentrales Autorisierungsterminal (ZAT) mit dem Sicherheitsmodul SM2.

Für den Benutzer sind die Komponenten Chipkarte und Chipkartenterminal bzw. Chipkartenleser relevant, über die die Verbindung zur Datensichtstation hergestellt wird.

An einem Chipkartenterminal kann der Systemzugang mit und ohne Überprüfung der PIN erfolgen. Es besitzt:

- eine Aufnahmeöffnung für die Chipkarte,
- ein Display für die Ausgabe von Meldungen,
- eine numerische Tastatur für die Eingabe der PIN,
- vier Funktionstasten:
  - Abschluß der PIN-Eingabe,
  - Abbruch eines Vorgangs und Auswurf der Chipkarte,
  - Korrektur der PIN-Eingabe und
  - Durchführen einer PIN-Änderung unabhängig vom Betriebssystem.

Der Chipkartenleser ist für den Systemzugang ohne Überprüfung der PIN vorgesehen. Es gibt ihn in zwei Ausführungen:

- eingebaut in die Datensichtstation oder
- als eigenständiges Gerät, das an die Datensichtstation angeschlossen wird.

Ein Chipkartenleser besitzt nur eine Aufnahmeöffnung für die Chipkarte, jedoch kein Display und keine eigene Tastatur.

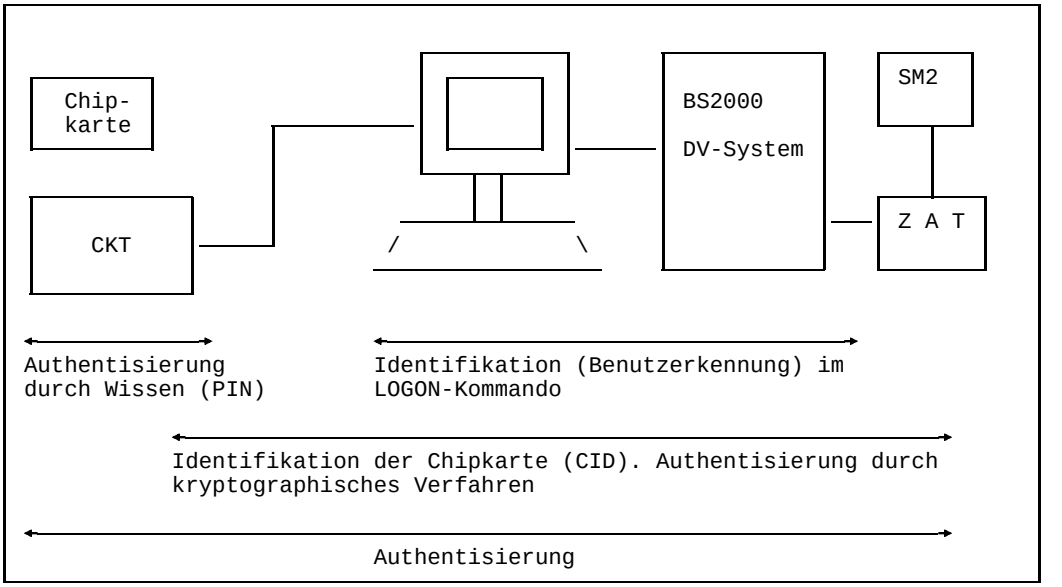


Bild 3: Systemkonfiguration für den Einsatz der Chipkarte

Funktionsweise des Chipkartensystems

Bei einem Systemzugang mittels Chipkarte mit Überprüfung der PIN findet zuerst eine Authentisierung des Benutzers gegenüber der Chipkarte und anschließend eine interne Authentisierung der Chipkarte gegenüber dem BS2000 statt (siehe Bild 3).

1) Authentisierung des Benutzers

   Die Chipkarte verlangt von ihrem Benutzer den Nachweis, daß er ihr rechtmäßiger Besitzer ist. Dazu muß er innerhalb einer vorgegebenen Zeitschranke die in der Chipkarte gespeicherte PIN am CKT eingeben. Die PIN hat eine Länge von 4 bis 12 Ziffern. Aus Sicherheitsgründen wird am Display des CKT für jede eingegebene Ziffer ein '*' angezeigt.

   Die Chipkarte befindet sich im Grundzustand, wenn die letzte Eingabe der aktuellen PIN korrekt war und die Chipkarte nicht gesperrt ist. Bei jeder Authentisierung des Benutzers mit einer Chipkarte im Grundzustand werden zwei Fehlversuche toleriert. Beim dritten Fehlversuch in Folge sperrt sich die Chipkarte. Sie kann nur wenige Male von der Benutzerverwaltung reaktiviert werden. Die Prüfung der PIN verhindert, daß die Karte bei Verlust oder Diebstahl mißbräuchlich verwendet wird. Da die Prüfung lokal zwischen Chipkarte und CKT stattfindet, ist ein Abhören von Informationen nicht möglich.

2) Authentisierung der Chipkarte

   Bei jedem Systemzugang verifiziert das BS2000, ob die Chipkarte, die in das CKT eingesteckt wurde, für die Benutzerkennung zugelassen ist, die im LOGON-Kommando eingegeben wurde. Nach der Übertragung der Chipkarten-Identifikationsnummer (CID) vom CKT an das BS2000 wird eine jedesmal wechselnde, nicht vorhersehbare Nachricht zwischen dem BS2000 und dem CKT ausgetauscht. Die dabei eingesetzten Algorithmen mit den zur Anwendung kommenden Verschlüsselungsverfahren garantieren den sicheren Authentisierungsvorgang.

   Bei einem Systemzugang mittels Chipkarte ohne Überprüfung der PIN findet nur die interne Authentisierung der Chipkarte gegenüber dem BS2000 statt.

Änderung der PIN

Die PIN läßt sich durch ein einfaches Verfahren jederzeit ändern. Um unbefugte Änderungen zu vermeiden, ist auch die Kenntnis der aktuellen PIN erforderlich. Die Änderung der PIN muß innerhalb einer vorgegebenen Zeitschranke erfolgen.

Vor der ersten Verwendung muß jede Chipkarte von der Systemverwaltung personalisiert werden, d.h. die Chipkarte wird dem Systemzugang in den Zugangsklassen DIALOG oder OPERATOR-ACCESS-TERMINAL und einer bestimmten Person zugeordnet. Zusätzlich wird in der Chipkarte gespeichert, ob besh im Systemzugang eine Überprüfung der PIN stattfindet. Danach wird sie evtl. mit einer Initialisierungs-PIN dem vorgesehenen Benutzer ausgehändigt.

4.2.4 Weitere Einschränkungen des Systemzugangs

Zum Schutz der Benutzerkennungen bietet das BS2000 zusätzliche Zugangsschutzmechanismen an, die von der Benutzerverwaltung für eine Benutzerkennung durch das SET-LOGON-PROTECTION- bzw. MODIFY-LOGON-PROTECTION-Kommando (siehe Anhang A) in Kraft gesetzt werden können:

- die Begrenzung der Lebensdauer einer Benutzerkennung,
- die Sperrung einzelner Zugangsklassen für eine Benutzerkennung,
- die Einschränkung des Systemzugangs in der Zugangsklasse DIALOG auf bestimmte Anschlußstellen (z.B. für Datensichtstationen) und
- Zugriffslisten für Benutzerkennungen für den Systemzugang in der Zugangsklasse BATCH.

Begrenzung der Lebensdauer einer Benutzerkennung

Die Lebensdauer einer Benutzerkennung kann von der Benutzerverwaltung auf einen beliebigen Zeitraum begrenzt werden. Wird eine Begrenzung der Lebensdauer gewünscht, z.B. für die Dauer eines Projekts, so ist für die betreffende Benutzerkennung ein Verfallsdatum festzulegen.

Die Überprüfung des Verfallsdatums erfolgt für die Zugangsklassen DIALOG und OPERATOR-ACCESS-TERMINAL nach der Eingabe des LOGON-Kommandos, für die Zugangsklasse BATCH bei der Bearbeitung des ENTER-Kommandos bzw. des ENTER-Makros, für die Zugangsklasse REMOTE BATCH bei der Bearbeitung der LOGON-Karte.

Der Benutzer wird bei einem Systemzugang im Zeitraum von einem Monat vor Erreichen des Verfallsdatums durch eine entsprechende Warnung informiert. Nach Überschreiten des Verfallsdatums wird die Benutzerkennung gesperrt. Die katalogisierten Dateien bleiben erhalten.

Sperrung einzelner Zugangsklassen für eine Benutzerkennung

Für eine Benutzerkennung kann von der Benutzerverwaltung jede der Zugangsklassen DIALOG, BATCH, OPERATOR-ACCESS-TERMINAL, OPERATOR-ACCESS-PROGRAM und REMOTE BATCH separat gesperrt werden.

Die Überprüfung der Sperrung erfolgt für die Zugangsklassen

DIALOG und OPERATOR-ACCESS-TERMINAL	nach der Eingabe des LOGON-Kommandos,
BATCH	bei der Bearbeitung des ENTER-Kommandos bzw. des ENTER-Makros

REMOTE BATCH	bei der Bearbeitung der LOGON-Karte
OPERATOR-ACCESS-PROGRAM	beim Zugang des programmierten Operators zur Anwendung $CONSOLE.

Der Benutzer wird durch eine Systemmeldung informiert, wenn er versucht unter einer Benutzerkennung in einer gesperrten Zugangsklasse Systemzugang zu erhalten.

Einschränkung des Systemzugangs auf bestimmte Anschlußstellen

Der Systemzugang in der Zugangsklasse DIALOG kann von der Benutzerverwaltung auf bestimmte Anschlußstellen eingeschränkt werden. Damit ist die Möglichkeit gegeben, ein LOGON-Kommando für besonders sensitive Benutzerkennungen nur von bestimmten Anschlußstellen aus zu gestatten.

Zugriffslisten für die Verwendung von Benutzerkennungen

Zugriffslisten für Benutzerkennungen können von der Benutzerverwaltung für die Zugangsklasse BATCH festgelegt werden. In einer Zugriffsliste für eine Benutzerkennung sind alle Benutzerkennungen vermerkt, die unter dieser Benutzerkennung Stapelaufträge starten dürfen.

Schutz der Zugangsklassen

Zum Schutz der Zugangsklassen DIALOG, BATCH OPERATOR-ACCESS-TERMINAL, OPERATOR-ACCESS-PROGRAM und REMOTE BATCH folgende Zugangsschutzmechanismen verwendet werden:

1) Kennwortverfahren,
2) Kennwort-Verschlüsselung,
3) Minimale Länge eines Kennworts,
4) Minimale Komplexität eines Kennworts,
5) Begrenzung der Lebensdauer eines Kennworts und
6) Begrenzung der Lebensdauer einer Benutzerkennung

in gleicher Weise angewendet werden. Die übrigen Zugangsschutzmechanismen sind nur für eine bestimmte Zugangsklasse gültig.

Spezifische Schutzmöglichkeiten für die Zugangsklasse DIALOG:

7) Chipkartenverfahren,
8) Sperrung der Zugangsklasse DIALOG,
9) Einschränkung auf bestimmte Anschlußstellen.

Spezifische Schutzmöglichkeiten für die Zugangsklasse BATCH:

7) Sperrung der Zugangsklasse BATCH,
8) Zugriffslisten.

Spezifische Schutzmöglichkeit für die Zugangsklasse REMOTE BATCH:

7) Sperrung der Zugangsklasse REMOTE BATCH.

Spezifische Schutzmöglichkeit für die Zugangsklasse OPERATOR-ACCESS-TERMINAL:

7) Chipkartenverfahren,
8) Sperrung der Zugangsklasse OPERATOR-ACCESS-TERMINAL

Spezifische Schutzmöglichkeit für die Zugangsklasse OPERATOR-ACCESS-PROGRAM:

7,8) Sperrung der Zugangsklasse OPERATOR-ACCESS-PROGRAM

4.3 Sicherer Zugang zum BS2000 in der Zugangsklasse DIALOG

Der prinzipielle Ablauf des Zugangs zum BS2000 in der Zugangsklasse DIALOG gliedert sich in zwei Schritte:

– die Durchführung des Prädialogs und
– die Eingabe des LOGON-Kommandos.

Der Prädialog initiiert den Aufbau einer Verbindung zwischen einer Datensichtstation und dem BS2000. Das LOGON-Kommando liefert die Eingaben zur Identifizierung und Authentisierung des Benutzers.

4.3.1 Prädialog

Im Prädialog müssen entsprechend dem aktuellen Zustand der Datensichtstation der Reihe nach folgende Schritte durchgeführt werden:

Fall 1: Die Datensichtstation ist ausgeschaltet

1) Datensichtstation einschalten
   Die Anzeigen LTG und TAST erscheinen am Bildschirm.
2) Taste (DUE) betätigen
   Die Anzeige CN01 PLEASE ENTER NET COMMAND erscheint am Bildschirm.
3) Taste (LSP) betätigen, um den Bildschirmspeicher zu löschen
4) Kommando ::opncon
   zum Aufbau der Verbindung eingeben (Voraussetzung ist, daß die Zeichenfolge '::' als Umschaltindikator festgelegt wurde.)

Der erfolgreiche Aufbau der Verbindung wird durch eine Systemmeldung auf dem Bildschirm angezeigt (Der genaue Text der Meldung ist abhängig von der Version des Betriebssystems.):

```
CN04 CONNECTED WITH $DIALOG,08/15;IND='::'
% JMS0150 INSTALLATION '7.590- G', BS2000 VERSION 'V110', HOST 'X123YZ45':
PLEASE LOGON OR SET LOGON PARAMETERS OR?
```

wobei:

CN04	Bezeichnung der Systemmeldung
$DIALOG	Bezeichnung der Anwendung
08/15	Prozessor- und Regionsnummer der Systemeinheit
IND='::'	Umschaltindikator

Durch Eingabe des Umschaltindikators '::' und des CLSCON-Kommandos in der Form '::clscon' kann die Verbindung zum BS2000 jederzeit wieder abgebrochen werden.

%	Meldungskennzeichen
JMS0150	Bezeichnung der Systemmeldung
7.590-G	Typ der Anlage
V110	Version des Betriebssystems (V11.0)
X123YZ45	Bezeichnung des Rechners

Fall 2: Die Datensichtstation ist eingeschaltet

Die Anzeigen LTG und TAST müssen vorhanden sein. Es sind die Schritte (2) bis (4) wie bei einer nicht eingeschalteten Datensichtstation auszuführen.

Vor allem bei eingeschalteten Datensichtstationen ist die Gefahr von LOGON-Fallen gegeben (siehe Seite 44).Deshalb sollte das Drücken der (LSP)-Taste und das Voranstellen des Umschaltindikators beim OPNCON-Kommando nicht unterlassen werden.

Sonderfall: Die Verbindung existiert bereits

Nach der Eingabe des OPNCON-Kommandos erscheint die Ausgabe CN06 ALREADY CONNECTED
Die Verbindung ist abzubrechen - sofern bei der Anmeldung kein anderer Umschaltindikator festgelegt wurde, kann dies mit dem Kommando ::clscon gesehen. Anschließend kann mit dem OPNCON-Kommando die Verbindung korrekt aufgebaut werden.

4.3.2 Identifizierung und Authentisierung mittels Kennwort

Ist eine Benutzerkennung durch das Kennwortverfahren geschützt, wird nach erfolgreichem Aufbau der Verbindung zum BS2000 die Identifizierung und Authentisierung des Benutzers durchgeführt. Das LOGON-Kommando beinhaltet folgende Eingaben, wobei jede Eingabe mit der Taste (DUE) abgeschlossen werden muß:

1) Identifizierung

   Das LOGON-Kommando (siehe Beispiel Seite 42) sollte in folgender Form eingegeben werden:

   .jobname logon userid,abrechnr

   wobei gilt:

   jobname : Auftragsname (optional)
   userid : Benutzerkennung
   abrechnr : Abrechnungsnummer

Hinweis

Das LOGON-Kommando erlaubt auch die direkte Eingabe eines Kennworts als weiteren Operanden. Diese Form der Kennworteingabe sollte aus Sicherheitsgründen aber vermieden werden, da sie nicht dunkelgesteuert erfolgt.

2) Authentisierung

   Das BS2000 fordert die Eingabe eines Kennworts:

   % JMS0151 PLEASE ENTER PASSWORD

   Die Eingabe erfolgt dunkelgesteuert, d.h. die eingegebenen Zeichen werden nicht auf dem Bildschirm dargestellt.

   Sind alle Eingaben richtig, meldet das BS2000 den erfolgreichen Zugang. Aus der Systemmeldung geht das aktuelle Datum und die Auftragsnummer hervor, unter der das BS2000 den Auftrag des Anwenders und die an die Benutzerkennung geknüpften Privilegien und Rechte verwaltet (TSN = Task Sequence Number). Darüber hinaus können weitere wichtige Systemdaten wie die Version des Betriebssystems, wichtige Telefonnummern oder verfügbare Software-Komponenten angezeigt werden (siehe Beispiel Seite 42).

   Im Anschluß an die Systemmeldung erscheint das BS2000-Prompting; es können nun Betriebssystem-Kommandos eingegeben werden. Rechenzentrumspezifisch kann vor der Ausgabe des BS2000-Prompting noch eine systemglobale oder eine benutzerspezifische LOGON-Prozedur ablaufen, die z.B. zusätzliche Sicherheitsfunktionen enthält.

   Bei jeder falschen Eingabe fordert das BS2000 zu einer vollständigen Wiederholung des LOGON-Kommandos auf. Dabei werden Zeit- und Wiederholungsstrafen verhängt:

   – Nach jeder falschen Eingabe kann 10 Sekunden lang keine weitere Eingabe erfolgen.
   – Nach der Eingabe von fünf falschen LOGON-Kommandos hintereinander wird die Verbindung zur Datensichtstation abgebrochen. Die Verbindung muß dann, beginnend mit dem Prädialog, neu aufgebaut werden.

Änderung des Kennworts

In besonderen Fällen ist sofort nach erfolgreichem LOGON-Kommando eine Änderung des Kennworts sinnvoll:

– Das LOGON-Kommando wird zum ersten Mal unter einer Benutzerkennung ausgeführt.

Beim Einrichten wird eine Benutzerkennung durch ein von der Benutzerverwaltung festgelegtes Kennwort geschützt. Dieses Kennwort sollte sofort nach der ersten Eingabe des LOGON-Kommandos durch ein Kennwort des Benutzers ersetzt werden, da auch die Benutzerverwaltung im laufenden Betrieb keine Kenntnis der aktuellen Kennwörter der Benutzer besitzen soll.

– Die Lebensdauer des Kennworts droht abzulaufen.
– Es besteht der Verdacht, daß eine unberechtigte Person Kenntnis des aktuellen Kennworts erlangt hat.

Die Änderung des Kennworts erfolgt mit dem Kommando MODIFY-USER-PROTECTION (siehe Anhang A). Bei Menüsteuerung ist das aktuelle Kennwort und das neue Kennwort einzugeben. Alle Eingaben erfolgen dunkelgesteuert. Sind die Eingaben richtig, so wird das Kennwort geändert, ohne daß die Änderung durch eine Systemmeldung bestätigt wird. Ist die Eingabe des aktuellen Kennworts falsch, so wird das aktuelle Kennwort nicht geändert. In diesem Fall gibt das BS2000 eine entsprechende Systemmeldung auf dem Bildschirm aus. Wurde bei der Generierung des BS2000 Kennwort-Verschlüsselung vereinbart, wird das neue Kennwort verschlüsselt im Betriebssystem abgespeichert.

4.3.3 Identifizierung und Authentisierung mittels Chipkarte

Ist eine Benutzerkennung für die Zugangsklasse DIALOG durch das Chipkartenverfahren geschützt, sind noch weitere Schritte auszuführen. Die Identifizierung und Authentisierung kann mit und ohne Überprüfung der PIN erfolgen. Meldungstexte, die bei einem korrekten Vorgehen am Bildschirm der Datensichtstation bzw. am Display des CKT ausgegeben werden, sind selbsterklärend (siehe Beispiele 2 und 3 Seite 43). Jede Eingabe der PIN erfolgt über die Tastatur des CKT und wird mit der dafür vorgesehenen Funktionstaste bestätigt. Jedes Zeichen der PIN wird am Display des CKT durch einen '*' ersetzt.

1) Identifizierung - Einstecken der Chipkarte in die Aufnahmeöffnung des CKT

   Die Chipkarte wird mit der Beschriftung nach oben in Richtung des aufgedruckten Pfeils korrekt eingesteckt.

2) Authentisierung- Eingabe der PIN

   Nach der Eingabe der korrekten PIN und einer erfolgreichen Überprüfung der Chipkarte durch das BS2000 erscheint am Bildschirm die Bestätigung des Systemzugangs analog zur Authentisierung mittels Kennwort. Nach erfolgreicher Authentisierung kann die Chipkarte aus dem CKT entnommen werden.

Änderung der PIN

Die PIN sollte in jedem Fall geändert werden, wenn die Chipkarte zum ersten Mal benutzt wird; sie sollte geändert werden, wenn eine andere Person Kenntnis von der PIN oder einzelnen Ziffern der PIN erlangt haben könnte. Nach der Aktivierung des CKT und dem Einstecken der Chipkarte in die Aufnahmeöffnung des CKT sind folgende Schritte der Reihe nach durchzuführen:

1) Drücken der Funktionstaste zur PIN-Änderung
2) Eingabe der alten (=aktuellen) PIN
3) Eingabe der neuen PIN
4) Nochmalige Eingabe der neuen PIN zur Bestätigung
5) Freigabe der Chipkarte durch Drücken der entsprechenden Funktionstaste

Die erfolgreiche Änderung der PIN wird am Display durch eine Meldung bestätigt.

4.3.4 Fehlerfälle beim Zugang mit Chipkarte

Verwendung einer gesperrten Chipkarte beim Zugang zum BS2000

Meldung am Display: `TOO MANY WRONG INPUTS! INCORRECT PIN INPUT`
Maßnahme: Benachrichtigung der Benutzerverwaltung

Falsches Einstecken der Chipkarte beim Zugang zum BS2000

Meldung am Display: `PLEASE SLIDE IN CHIP CARD CORRECTLY`

Falsche Eingabe der aktuellen PIN beim Zugang zum BS2000

Mit der Chipkarte im Grundzustand (siehe Seite 30ff) werden zwei Fehlversuche bei der Eingabe einer aktuellen PIN toleriert.

Meldung am Display: `RETRY PIN INPUT`

Nach drei Fehlversuchen wird die Chipkarte gesperrt.

Meldung am Display: `TOO MANY WRONG INPUTS! INCORRECT PIN INPUT`
Maßnahme: Benachrichtigung der Benutzerverwaltung

Falsche Eingabe der aktuellen PIN bei der PIN-Änderung

Mit der Chipkarte im Grundzustand (siehe Seite 30ff) werden zwei Fehlversuche bei der Eingabe einer zu ändernden PIN toleriert.

Meldung am Display: `PIN-EINGABE WIEDERHOLEN`

Nach drei Fehlversuchen wird die Chipkarte gesperrt.

Meldung am Display: `ZU VIELE FEHLEINGABEN! PIN-EINGABE UNZULÄSSIG`
Maßnahme: Benachrichtigung der Benutzerverwaltung

Zeitüberschreitung beim Zugang zum BS2000

Meldungen am Display: `TIMEOUT`
Maßnahme: Wiederholung des Zugangsverfahrens

Zeitüberschreitung bei der PIN-Änderung

Meldungen am Display: `ZEIT FÜR PIN-EINGABE ABGELAUFEN`
Maßnahme: Wiederholung der PIN-Änderung

Falsche Bestätigung der neuen PIN bei der PIN-Änderung

Meldung am Display: `NEUE PIN FALSCH`
Maßnahme: Wiederholung der PIN-Änderung

Anmerkung

Beim Zugang zum BS2000 erfolgt die Ausgabe der Meldungen am Display des CKT in der gleichen Sprache wie die Ausgabe der Meldungen am Bildschirm der Datensichtstation. Bei der Änderung einer PIN werden deutsche Meldungstexte ausgegeben.

Beispiele

Beispiel 1: Prädialog und Zugangskontrolle mit Kennwort

```
 CN01 PLEASE ENTER NET COMMAND                                              1)
 ::opncon                                                                   2)
 CN04 VERBUNDEN MIT $DIALOG,08/15;IND='::'                                  3)

JMS0150 INSTALLATION '  H90-P', BS2000 VERSION 'V110', HOST 'D015ZE08':
PLEASE ENTER '/SET-LOGON-PARAMETERS' OR '?'
/set-logon-parameters user=hannibal,account=12345678,jobname=security  4)
%  JMS0151 PLEASE ENTER PASSWORD                                           5)
                                                                           6)

  JMS0066 JOB 'SECURITY' ACCEPTED ON 92-11-26 AT 12:19, TSN = 2CX1     7)
*********************************************************************  8)
***  ANLAGE 7.582P-0250                  BS2000   V11.0A      ***
***                                      SPOOL    V2.7A       ***
*** SYSTEMBETREUUNG  TEL. 44444           FT-BS2   V5.0        ***
***                  TEL. 55555           VM2000   V2.0A00     ***
*** ANLAGENTELEFON   TEL. 66666                                 ***
*** DRUCKERZENTRUM   TEL. 77777   ANRUFBEANTW. BS2  TEL. 99999 ***
*** NETZADMIN.       TEL. 88888   ANRUFBEANTW. NETZ TEL. 22222 ***
***                                                            ***
*********************************************************************
 % CMD0553 SDF IS AVAILABLE. FOR FURTHER INFORMATION ENTER /HELP-SDF
 /                                                                         9)
```

1) Der Benutzer wird aufgefordert, den Prädialog zu führen.
2) Durch Eingabe des OPNCON-Kommandos wird eine Verbindung von der Datensichtstation zum BS2000 aufgebaut.
3) Der erfolgreiche Aufbau der Verbindung wird am Bildschirm angezeigt, und es wird zur Eingabe des LOGON-Kommandos aufgefordert.
4) Das LOGON-Kommando wird eingegeben. Der Auftragsname lautet **security**, die Benutzerkennung **hannibal** und die Abrechnungsnummer **12345678.**
5) Der Benutzer wird zur Eingabe des Kennworts aufgefordert.
6) Die Eingabe des Kennworts erfolgt dunkelgesteuert.
7) Nach erfolgreicher Eingabe des Kennworts erscheint eine Meldung des Betriebssystems, aus der Datum und Zeit des Systemzugangs sowie die Auftragsnummer (TSN) ersichtlich sind.
8) Es folgen Informationen der Systemverwaltung.
9) Durch das BS2000-Prompting wird angezeigt, daß das Betriebssystem bereit ist, weitere Kommandos entgegenzunehmen.

Beispiel 2: Prädialog und Zugangskontrolle mit Kennwort, Chipkarte und Überprüfung der PIN

```
  CN01 PLEASE ENTER NET COMMAND                                          1)
  ::opncon                                                               2)
CN04 VERBUNDEN MIT $DIALOG,08/15;IND='::'                                3)

 JMS0150 INSTALLATION '  H90-P', BS2000 VERSION 'V110', HOST 'D015ZE08':
 PLEASE ENTER '/SET-LOGON-PARAMETERS' OR '?'
 /set-logon-parameters user=hannibal,account=12345678,jobname=security  4)
 %  JMS0151 PLEASE ENTER PASSWORD                                       5)
                                                                        6)
  CHC0100 PLEASE SLIDE IN CHIP CARD                                    7)

  PLEASE SLIDE IN CHIP CARD                                             8)
  PLEASE ENTER PIN                                                      9)
                                                                       10)

   JMS0066 JOB 'SECURITY' ACCEPTED ON 92-11-26 AT 12:19, TSN = 2CX1    11)
 ********************************************************************  12)
 ***  ANLAGE 7.582P-0250                  BS2000   V11.0A      ***
 ***                                      SPOOL    V2.7A       ***
 *** SYSTEMBETREUUNG  TEL. 44444          FT-BS2   V5.0        ***
 ***                  TEL. 55555          VM2000   V2.0A00     ***
 *** ANLAGENTELEFON   TEL. 66666                               ***
 *** DRUCKERZENTRUM   TEL. 77777   ANRUFBEANTW. BS2  TEL. 99999 ***
 *** NETZADMIN.       TEL. 88888   ANRUFBEANTW. NETZ TEL. 22222 ***
 ***                                                           ***
 ********************************************************************
  % CMD0553 SDF IS AVAILABLE. FOR FURTHER INFORMATION ENTER /HELP-SDF
  /                                                                    13)
```

1) Der Benutzer wird aufgefordert, den Prädialog zu führen.
2) Durch Eingabe des OPNCON-Kommandos wird eine Verbindung von der Datensichtstation zum BS2000 aufgebaut.
3) Der erfolgreiche Aufbau der Verbindung wird am Bildschirm angezeigt, und es wird zur Eingabe des LOGON-Kommandos aufgefordert.
4) Das LOGON-Kommando wird eingegeben. Der Auftragsname lautet **security**, die Benutzerkennung **hannibal** und die Abrechnungsnummer **12345678.**
5) Der Benutzer wird zur Eingabe des Kennworts aufgefordert.
6) Die Eingabe des Kennworts erfolgt dunkelgesteuert.
7) Der Benutzer wird zum Einlegen der Chipkarte in die Aufnahmeöffnung des CKT aufgefordert. Die Meldung erscheint am Bildschirm der Datensichtstation.
8) Die Meldung erscheint am Display des CKT.
9) Die Meldung erscheint am Display des CKT. Der Benutzer muß die aktuelle PIN an der Tastatur des CKT eingeben.
10) Jede Ziffer der PIN wird am Display des CKT durch einen '*' ersetzt.
11) Nach erfolgreicher Eingabe der PIN und erfolgreicher Überprüfung der Chipkarte durch das BS2000 erscheint eine Meldung des Betriebssystems, aus der Datum und Zeit des Systemzugangs sowie die Auftragsnummer (TSN) ersichtlich sind.
12) Es folgen Informationen der Systemverwaltung.
13) Durch das BS2000-Prompting wird angezeigt, daß das Betriebssystem bereit ist, weitere Kommandos entgegenzunehmen.

Beispiel 3: Änderung der PIN

Nach der Aktivierung des CKT, dem korrekten Einstecken der Chipkarte in die Aufnahmeöffnung des CKT und nach dem Drücken der Funktionstaste zur PIN-Änderung ergibt sich folgender Ablauf:

BITTE ALTE PIN EINGEBEN

BITTE NEUE PIN EINGEBEN

NEUE PIN ZUR BESTÄTIGUNG EINGEBEN

PIN-ÄNDERUNG ERFOLGREICH

Alle Meldungen erscheinen am Display des CKT. Jede Eingabe der PIN erfolgt über die Tastatur des CKT. Jede Ziffer der PIN wird am Display durch einen '*' ersetzt.

4.3.5 LOGON-Fallen

Besondere Vorsicht ist geboten, wenn ein Benutzer eine bereits eingeschaltete Datensichtstation vorfindet. Es besteht dann nämlich die Gefahr, daß unbemerkt vom Benutzer ein Programm gestartet wurde, das den Grundzustand der Datensichtstation vortäuscht und anschließend den Systemzugang detailliert nachbildet, mit der Absicht Systemzugangsdaten zu erfahren.

Programme, die den Systemzugang nachbilden, erzeugen einen Bildschirm, wie er vom Zustand der Datensichtstation vor dem Verbindungsaufbau bekannt ist. Der Ablauf der Zugangskontrolle wird jedoch durch das Programm simuliert. Das Programm fängt dabei alle eingegebenen Daten ab, also alle zum Systemzugang relevanten Daten. Nach erfolgreichem Ausspähen der Information kann das Programm mit einer Fehlermeldung terminieren. Der Benutzer erhält so den Eindruck, in der vorangegangenen Eingabe einen Fehler gemacht zu haben. Das eigentliche Ausspähen durch das Programm bleibt unentdeckt.

Zur Verhinderung von LOGON-Fallen sollte deshalb unbedingt beachtet werden, daß zum Aufbau der Verbindung jeder einzelne der Schritte (1)-(4) entsprechend Abschnitt "Prädialog", Seite 36 ausgeführt wird.

4.4 Organisatorische Maßnahmen des Benutzers zur Ergänzung des Zugangsschutzes

Regeln für den Umgang mit Identifizierungs- und Authentisierungsdaten

- Sämtliche schriftlichen Unterlagen, aus denen Rückschlüsse auf Zugangsmöglichkeiten zum System gezogen werden können, sollten sorgfältig und für Unbefugte unzugänglich aufbewahrt werden.
- Programmierbare Tasten sollten niemals mit den Zugangsdaten (Benutzerkennung, Abrechnungsnummer, Kennwort) oder sonstigen sicherheitsrelevanten Daten belegt werden.
- Kenntnis von sicherheitsrelevanten Daten sollten nur diejenigen Personen erhalten, die diese unbedingt für ihre Arbeit benötigen.

Regeln für den Umgang mit Kennwörtern

Kennwörter bieten nur solange einen wirksamen Schutz, wie sie lediglich dem autorisierten Benutzer bekannt sind. Deshalb sollten folgende Regeln für den Umgang mit Kennwörtern beachtet werden:

- Um die Erratbarkeit zu erschweren, sollten möglichst Pseudowörter verwendet werden, die nicht Wörterbüchern oder Lexika entstammen. Zusätzliche Ziffern und Sonderzeichen machen das Erraten eines Kennworts nahezu unmöglich.
- Kennwörter sollten möglichst lang gewählt werden.
- Kennwörter sollten nie aufgeschrieben werden.
- Kennwörter sollten nicht in Dateien abgelegt werden.
- Kennwörter, die in irgendeinem Zusammenhang mit dem Privatleben stehen (z.B. der persönliche Name, die Namen von Familienangehörigen, Haustieren, Automarken, Autokennzeichen, Städtenamen etc.) oder in einem Zusammenhang mit dem Unternehmen oder der Tätigkeit innerhalb des Unternehmens stehen (z.B. Namen von Abteilungen, Projekten etc.), sollten vermieden werden.
- Zusätzlich zu den Regeln für den Umgang mit Kennwörtern sollten die Hinweise zu LOGON-Fallen beachtet werden.

Regeln für den Umgang mit Chipkarten

Für Chipkarten gilt in gleicher Weise, daß der Schutz nur solange wirksam ist, wie die PIN nur dem autorisierten Benutzer bekannt ist. Folgende Hinweise sollten daher beachtet werden:

- Die Chipkarte sollte sorgfältig aufbewahrt werden.
- Die PIN sollte nicht schriftlich festgehalten werden. Ist ihre schriftliche Aufzeichnung dennoch unvermeidbar, sollten Chipkarte und PIN-Aufzeichnung niemals am gleichen Ort aufbewahrt werden. Auf jeden Fall darf die PIN niemals auf der Chipkarte notiert werden! Die PIN-Aufzeichnung sollte dann sicher verschlossen werden.

- Die PIN sollte in keinem Zusammenhang mit dem Privatleben oder der Tätigkeit in der Firma stehen.
- Für die Eingabe der PIN sollten nach Möglichkeit nur bekannte Geräte benutzt werden.
- Bei der Eingabe der PIN sollte eine Beobachtung ausgeschlossen werden.
- Die PIN sollte in regelmäßigen Zeitabständen geändert werden.
- Beim Verdacht, daß eine unbefugte Person Kenntnis der PIN oder von einzelnen Ziffern der PIN erlangt haben könnte, sollte die PIN sofort geändert werden.

Regeln beim Verlassen des Arbeitsplatzes

Verläßt der Benutzer seinen Arbeitsplatz an einer Datensichtstation während des Dialogs mit dem BS2000, so sind sämtliche nicht explizit durch Kennwörter geschützte Dateien vor Mißbrauch durch unbefugte Personen nicht mehr gesichert. Deshalb sollte - auch bei kurzzeitiger Abwesenheit - der Dialog mit dem LOGOFF-Kommando beendet werden.

Für die Eingabe des LOGOFF-Kommandos sollten folgende Regeln beachtet werden:

- Der Bildschirm der Datensichtstation sollte durch Drücken der entsprechenden Taste gelöscht werden.
- Das LOGOFF-Kommando sollte in jedem Fall eingegeben werden (evtl. mit weiteren Operanden, siehe die Beschreibung des LOGOFF-Kommandos im Anhang A).
- Die Bestätigung des LOGOFF-Kommandos sollte abgewartet werden.
- Bei Abwesenheit sollte die Datensichtstation in jedem Fall ausgeschaltet werden.

5 Benutzerorganisation, Benutzerrechte und Benutzerverwaltung

Neben der Identifizierung und Authentisierung der Benutzer und ihrer Zuordnung zu Benutzerkennungen ist die Strukturierung der Benutzerwelt eine wichtige Voraussetzung für wirksamen Zugriffsschutz. Das BS2000 ermöglicht eine hierarchische Organisation der Benutzer, die die Nachbildung bestehender Organisationsformen ebenso gestattet wie die projektorientierte Zusammenfassung von Benutzern.

Die Verwaltung der Benutzergruppen bezüglich der ihr zugeordneten Benutzerkennungen und deren Benutzerrechte kann erfolgen:

- dezentral durch Gruppenverwalter, um die Systemverwaltung zu entlasten, und
- zentral durch systemglobale Benutzerverwalter. Diese sind durch das Privileg USER-ADMINISTRATION zu einer privilegierten Durchführung der Benutzerverwaltung berechtigt.

Im vorliegenden Kapitel steht die Benutzerverwaltung durch Gruppenverwalter im Mittelpunkt der Betrachtungen. Einleitend werden das grundlegende Konzept der Benutzerorganisation des BS2000 sowie die Benutzerrechte erläutert.

5.1 Benutzerorganisation

Die Basis für die Organisation der Benutzer des BS2000 bildet das Konzept der Benutzergruppen.

5.1.1 Benutzergruppen

Eine Benutzergruppe des BS2000 bezeichnet die Zusammenfassung einzelner Benutzerkennungen. Jede Benutzergruppe wird - unabhängig von den Bezeichnungen der Benutzerkennungen, die sie bilden, - durch einen eindeutigen Gruppennamen, die Gruppenkennung, repräsentiert. Kennzeichnend für eine Benutzergruppe sind:

- die Gruppenmitglieder,
- der Gruppenverwalter,
- das Gruppenpotential an Benutzerrechten und
- die Gruppenbeschreibungsdaten.

Jede Benutzergruppe kann mehrere Untergruppen besitzen. Eine Untergruppe ist dabei immer genau einer übergeordneten Benutzergruppe zugeordnet. Eine Gruppenstruktur des BS2000 kann so hierarchisch ein- oder mehrstufig aufgebaut werden.

Die Wurzel einer Gruppenstruktur des BS2000 bildet die Universalgruppe. Sie besitzt keine Gruppenkennung und wird mit *UNIVERSAL bezeichnet. Die Universalgruppe ist in einem generierten BS2000 immer vorhanden und faßt alle vom Betriebssystem standardmäßig eingerichteten Benutzerkennungen zusammen (siehe Sicherheitshandbuch für die Systemverwaltung des BS2000 [12]). Nach der Generierung des BS2000 können der Universalgruppe Untergruppen und weitere Gruppenmitglieder zugeordnet werden. Für die Universalgruppe gibt es keine Einschränkungen bezüglich der verfügbaren Benutzerrechte.

Jede weitere Benutzergruppe muß explizit eingerichtet werden und ist immer die Untergruppe einer bereits bestehenden Benutzergruppe. Eine Gruppenstruktur ist stets an genau einen Pubset gebunden. In einem Multiple-Public-Volume-Set-System (MPVS-System) können mehrere unterschiedliche Gruppenstrukturen aufgebaut werden (siehe Seite 81)

Gruppenmitglieder

Jede Benutzerkennung des BS2000 ist genau einer Benutzergruppe als Gruppenmitglied zugeordnet. Einem Gruppenmitglied können Benutzerrechte zugewiesen werden.

Gruppenverwalter

Eine Benutzergruppe kann dezentral von einem Gruppenverwalter verwaltet werden. Der Gruppenverwalter wird in einem solchen Fall repräsentiert durch eine Benutzerkennung aus der Menge der Gruppenmitglieder, die die Benutzergruppe bilden. Jede Benutzergruppe hat höchstens einen Gruppenverwalter. Ist für eine Benutzergruppe kein Gruppenverwalter ernannt worden, so wird sie von einem hierarchisch übergeordneten Gruppenverwalter oder einem systemglobalen Benutzerverwalter verwaltet (siehe Seite 83). Die Ernennung zum Gruppenverwalter erfolgt entweder durch den Gruppenverwalter einer bereits bestehenden, übergeordneten Benutzergruppe oder durch einen systemglobalen Benutzerverwalter.

Die Grundlage für die Verwaltung einer Benutzergruppe bilden eine Berechtigung zur Ausführung bestimmter Kommandos, ein Gruppenpotential an Benutzerrechten und die Gruppenbeschreibungsdaten (siehe Seite 66).

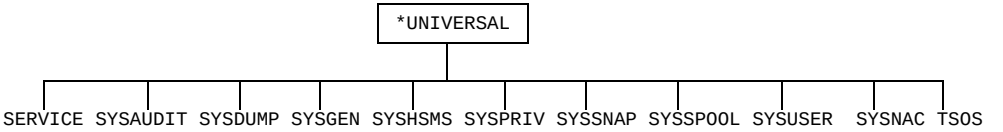
Anmerkungen

- Der Leser beachte, daß mit der Einführung von Benutzergruppen in das BS2000 ein eigenständiger Gruppenbegriff gewählt wurde. Eine Benutzergruppe wird also nicht durch eine Benutzerkennung repräsentiert, sondern bezeichnet eine Menge von Benutzerkennungen, für die unabhängig von ihren Elementen ein eindeutiger Name, die Gruppenkennung, festgelegt wird. Der Gruppenverwalter muß allerdings eine Benutzerkennung aus dieser Menge sein.
- Die Beschreibungen beziehen sich auf eine Benutzergruppenstruktur auf einem Pubset. In einem MPVS-System können auf unterschiedlichen Pubsets Benutzergruppen mit gleichen Gruppennamen existieren, die möglicherweise mit unterschiedlichen Gruppenmitgliedern oder Gruppenverwaltern ausgestattet sind. Die Verwaltung von Benutzerkennungen und Benutzergruppen erfolgt stets innerhalb eines Pubset (siehe Seite 81).
- Zur Ermittlung der Gruppenzugehörigkeit, z.B. bei der Zugriffsüberprüfung von Dateien und Jobvariablen, wird grundsätzlich die Benutzergruppenstruktur herangezogen, die auf dem Home-Pubset der laufenden BS2000-Sitzung aufgebaut ist.
- Benutzergruppenstrukturen, die auf Daten-Pubsets abgelegt sind, dienen lediglich dazu, pubset-spezifische Attribute (PUBLIC-SPACE-LIMIT, PUBLIC-SPACE-EXCESS) zu verwalten. Sie werden nicht für die Zugriffsüberprüfung herangezogen (siehe auch Seite 82).

5.1.2 Beispiele für Benutzergruppen

Beispiel 1: Initiale Gruppenstruktur

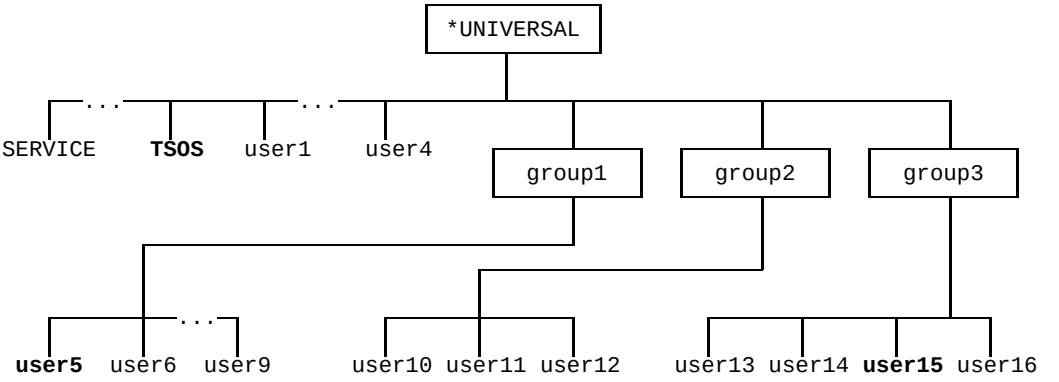
Die initiale Gruppenstruktur besteht aus einer Benutzergruppe, der Universalgruppe. Ihre Gruppenmitglieder sind alle vom Betriebssystem standardmäßig eingerichteten Benutzerkennungen (siehe Sicherheitshandbuch für die Systemverwaltung [12]).



Gruppenkennung	Gruppenmitglieder	Gruppenverwalter	Untergruppen
*UNIVERSAL	SERVICE SYSAUDIT SYSDUMP SYSGEN SYSHSMS SYSPRIV SYSNAC SYSSNAP SYSSPOOL SYSUSER TSOS	TSOS (systemglobaler Benutzerver- walter)	keine

Bild 4: Initiale Gruppenstruktur

Beispiel 2: Einstufige Gruppenstruktur

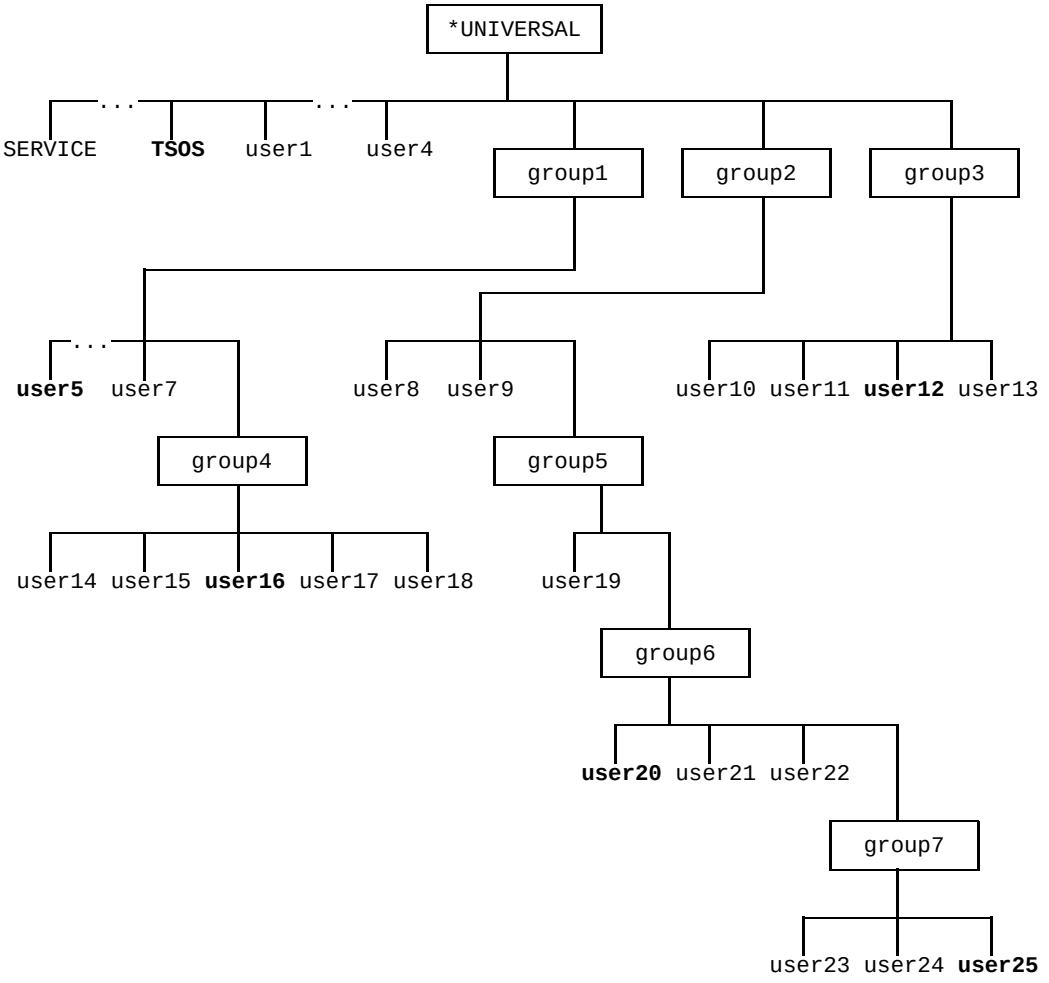


Struktur			Verwaltung
Gruppenkennung	Gruppenmitglieder	Untergruppen	Gruppenverwalter gruppen-:system- spezi- :global fisch :
*UNIVERSAL	SERVICE ... TSOS user1 user2 user3 user4	group1 group2 group3	- :TSOS : : : : : :
group1	user5 user6 user7 user8 user9	-	user5 :TSOS : : : :
group2	user10 user11 user12	-	- :TSOS : : :
group3	user13 user14 user15 user16	-	user15 :TSOS : : : :

Bild 5: Einstufige Gruppenstruktur

Legende: - Spalte "Untergruppen": Es ist keine Untergruppe definiert.
Spalte "Gruppenverwalter": Es ist kein gruppenspezifischer Gruppenverwalter definiert.

Beispiel 3: Mehrstufige Gruppenstruktur



Struktur			Verwaltung
Gruppenkennung	Gruppenmitglieder	Untergruppen	Gruppenverwalter gruppen-:system- spezi- :global fisch :
*UNIVERSAL	SERVICE ... TSOS user1 user2 user3 user4	group1 group2 group3	- : TSOS : : : : : :
group1	user5 user6 user7	group4	user5 : TSOS : : : :
group2	user8 user9	group5	: TSOS : : :
group3	user10 user11 user12 user13	-	user12 : TSOS : : : :
group4	user14 user15 user16 user17 user18	-	user16 : TSOS user5 : : : : :
group5	user19	group6	: TSOS :
group6	user20 user21 user22	group7	user20 : TSOS : : :
group7	user23 user24 user25	-	user25 : TSOS user20 : :

Bild 6: Mehrstufige Gruppenstruktur

Anmerkung:

Für alle Benutzergruppen, die über einen Gruppenverwalter verfügen, kann die Verwaltung durchgeführt werden:

- von diesem Gruppenverwalter,
- von einem hierarchisch übergeordneten Gruppenverwalter oder
- von einem systemglobalen Benutzerverwalter.

Für alle Benutzergruppen, die über keinen Gruppenverwalter verfügen, kann die Verwaltung durchgeführt werden:

- von einem hierarchisch übergeordneten Gruppenverwalter oder
- von einem systemglobalen Benutzerverwalter.

5.2 Benutzerrechte und Benutzerverwaltung

Über Benutzerrechte kann für Benutzerkennungen die Zuteilung von Systemdiensten und Betriebsmitteln unterschiedlich gestaltet und den Erfordernissen angepaßt werden. Beispielsweise kann durch Vergabe eines Benutzerrechts eine Benutzerkennung dazu berechtigt werden, mehr als den zugeteilten gemeinschaftlichen Speicherplatz in Anspruch zu nehmen.

Die Benutzerrechte werden eingeteilt in:

- allgemeine Benutzerrechte und
- das spezielle Benutzerrecht "Gruppenverwalterrecht" mit den drei Ausprägungen MANAGE-RESOURCES, MANAGE-MEMBERS und MANAGE-GROUPS.

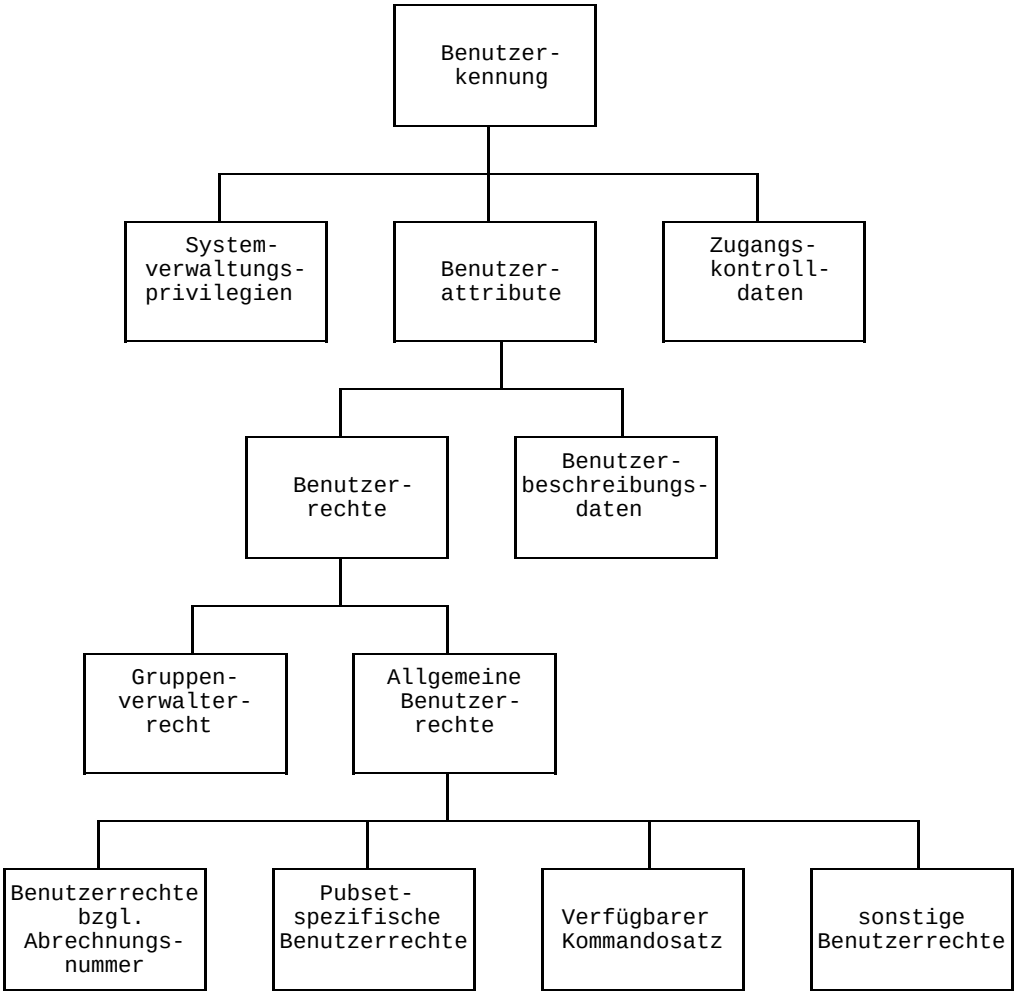


Bild 7: Merkmale einer Benutzerkennung

Die Benutzerverwaltung wird unterteilt in:

- die systemglobale Benutzerverwaltung (siehe Seite 83), die von Benutzern mit dem Privileg USER-ADMINISTRATION durchgeführt wird, und
- die gruppenspezifische Benutzerverwaltung (siehe Seite 66), die von Benutzern mit dem Gruppenverwalterrecht durchgeführt wird. Das Gruppenverwalterrecht gehört zum Potential einer Benutzergruppe und kann im Rahmen des Potentials nur einer Benutzerkennung der Benutzergruppe zugeteilt werden. Diese Benutzer werden auch als Gruppenverwalter bezeichnet. Im Gegensatz zu den allgemeinen Benutzerrechten ist das Gruppenverwalterrecht also nicht an eine Benutzerkennung, sondern an eine Benutzergruppe geknüpft.

Die systemglobale Benutzerverwaltung ist der Gruppenverwaltung übergeordnet. Insbesondere kann sie alle Benutzer und Benutzergruppen
verwalten und ihnen über das bestehende Gruppenpotential hinaus Benutzerrechte zuweisen. Die Systemverwalterrechte, die die Benutzerverwaltung beeinflussen, und die Benutzerrechte können (siehe Bild 8) hierarchisch geordnet werden.

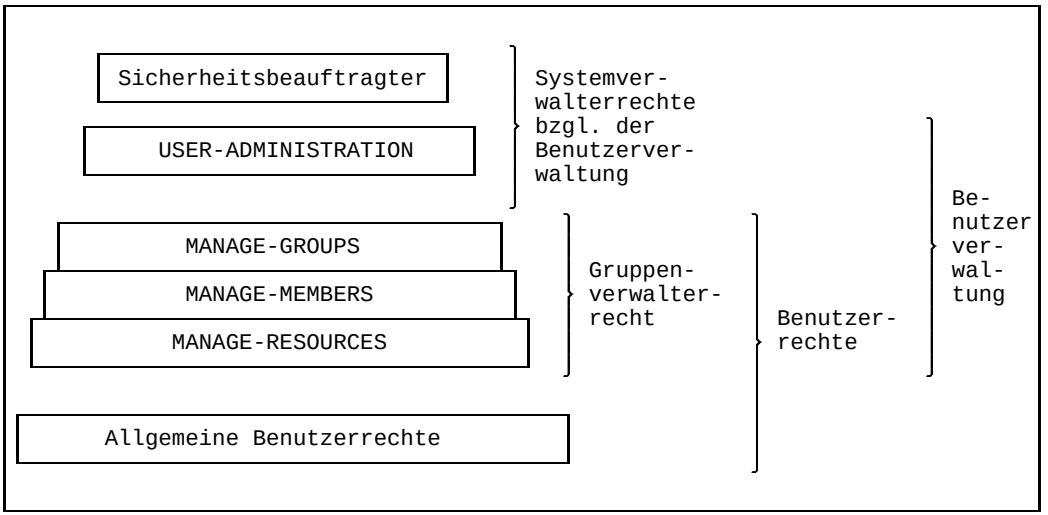


Bild 8: Hierarchische Beziehungen zwischen Benutzerrechten und Privilegien

Jede Benutzerkennung kann mit allgemeinen Benutzerrechten ausgestattet werden. Die Vergabe und der Entzug dieser Benutzerrechte wird von der Benutzerverwaltung durchgeführt, wobei die Gruppenverwaltung an die bestehende Gruppenstruktur und das Gruppenpotential gebunden ist.

Eine Sonderstellung nimmt der Sicherheitsbeauftragte ein. Ihm obliegt die Verwaltung der Systemverwalterrechte. Bei Auslieferung und nach einem First-Startup ist das Privileg SECURITY-ADMINISTRATION des Sicherheitsbeauftragten an die Kennung SYSPRIV vergeben. Das Privileg des Sicherheitsbeauftragten kann im laufenden Betrieb nicht an eine andere Kennung vergeben werden. Soll eine andere Kennung Sicherheitsbeauftragter werden, so muß diese neue Kennung über den STARTUP-PARAMETER-SERVICE eingestellt werden.

Der Sicherheitsbeauftragte beeinflußt die Benutzerverwaltung durch die Vergabe bzw. den Entzug des Systemverwalterrechts USER-ADMINISTRATION (siehe Sicherheitshandbuch für die Systemverwaltung des BS2000 [12]) und durch die Festlegung von Überwachungsaktionen über SAT (Security Audit Trail, Seite 168 [5]). Er kann jedoch keine Funktionen der Benutzerverwaltung, wie das Einrichten einer neuen Benutzerkennung etc., ausüben.

5.2.1 Allgemeine Benutzerrechte

Allgemeine Benutzerrechte werden für jede Benutzerkennung von der Benutzerverwaltung vergeben. Sie werden im Benutzerkatalog eines anzugebenden Pubset abgespeichert (siehe Seite 81) und können in drei Klassen eingeteilt werden:

- Benutzerrechte bezüglich der Abrechnungsnummer,
- pubset-spezifische Benutzerrechte und
- sonstige Benutzerrechte.

Im folgenden werden die einzelnen Benutzerrechte entsprechend dieser Unterteilung grob skizziert. Sofern nicht explizit erwähnt, werden sie mit den Kommandos ADD-USER bzw. MODIFY-USER (siehe Anhang A) vereinbart:

Benutzerrechte bezüglich der Abrechnungsnummer

ACCOUNT
Legt Abrechnungsnummern der Benutzerkennung fest.

MAX-ACCOUNT-RECORDS
Schränkt das Sammeln von benutzerspezifischen Abrechnungssätzen ein und vergibt die Berechtigung, eigene Abrechnungssätze mit eigener Satzkennung in die Abrechnungsdatei zu schreiben.

CPU-LIMIT
Legt die maximal verbrauchbare CPU-Zeit für die Aufträge des Benutzers fest.

PRIVILEGE
Vereinbart weitere Benutzerrechte:

- NO-CPU-LIMIT
  Der Benutzer erhält die Berechtigung, Stapelaufträge mit hoher Zeitbegrenzung ablaufen zu lassen.
- START-IMMEDIATE
  Der Benutzer ist berechtigt, die Job-Express-Funktion zu nutzen.
- INHIBIT-DEACTIVATION
  Aufträge des Benutzers können nicht deaktiviert werden.

SPOOLOUT-CLASS
Legt die Spoolout-Klasse der Benutzerkennung fest.

MAXIMUM-RUN-PRIORITY
Legt die höchste Priorität fest, die einer Task bei Bearbeitungsbeginn zugewiesen werden kann.

MAX-ALLOWED-CATEGORY
Legt die Kategorie fest, in der der Benutzer Aufträge führen darf.

Pubset-spezifische Benutzerrechte

FILE-NUMBER-LIMIT
Vereinbart die maximale Anzahl von Dateien, die angelegt werden dürfen.

JV-NUMBER-LIMIT
Vereinbart die maximale Anzahl von Job-Variablen, die angelegt werden dürfen.

PUBLIC-SPACE-LIMIT
Legt den maximal verbrauchbaren Speicherplatz auf dem zugewiesenen Pubset in PAM-Blöcken fest.

PUBLIC-SPACE-EXCESS
Vereinbart, ob der Benutzer die beim PUBLIC-SPACE-LIMIT definierte Grenze für den Speicherplatz auf dem zugewiesenen Pubset überschreiten darf.

TEMP-SPACE-LIMIT
Vereinbart den maximalen temporären Speicherplatz, der auf dem angegebenen, gemeinschaftlichen Datenträger belegt werden darf.

Sonstige Benutzerrechte

TAPE-ACCESS
Vereinbart, ob Fehlermeldungen bei Kennsatzprüfungen von Magnetbändern ignoriert werden dürfen.

FILE-AUDIT
Legt fest, ob der Benutzer Zugriffe auf seine Dateien mit SAT überwachen lassen kann (siehe Operand AUDIT im Kommando CREATE-FILE).

CSTMP-MACRO-ALLOWED
Vereinbart, ob der Benutzer in seinen Programmen den CSTMP-Makro verwenden darf.

TEST-OPTIONS
Legt die maximal mögliche Testprivilegierung fest und vereinbart, ob eine Änderung der Testprivilegierung durch den Benutzer mit oder ohne Kontrolle der Systembedienung erfolgt.

PROFILE-ID
Vereinbart den Eintrag in der SDF-Parameterdatei, unter dem der Name der Gruppensyntaxdatei hinterlegt ist. Wird dem Parameter PROFILE-ID kein Wert zugewiesen, gelten nur die Kommandos der Systemsyntaxdatei.

ADDRESS-SPACE-LIMIT
Legt den für die Benutzerkennung maximal zur Verfügung stehenden Benutzeradreßraum in Megabyte fest.

RESIDENT-PAGES
Legt die Anzahl der residenten Hauptspeicherseiten fest, die der Benutzer beanspruchen darf.

Neben den allgemeinen Benutzerrechten dienen Benutzerbeschreibungsdaten und Zugangskontrolldaten zur Beschreibung einer Benutzerkennung (siehe Bild 7). Die Benutzerbeschreibungsdaten werden mit den Kommandos ADD-USER bzw. MODIFY-USER festgelegt, die Zugangskontrolldaten mit den Kommandos SET-LOGON-PROTECTION bzw. MODIFY-LOGON-PROTECTION (siehe Anhang A). Drei Zugangskontrolldaten können über alle vier Kommandos festgelegt werden.

DMS-TUNING-RESOURCES
Vereinbart, welche Performance-Maßnahmen ergriffen und in welcher Form sie genutzt werden dürfen.

CODED-CHARACTER-SET
Gibt an, welches CODED-CHARACTER-SET (CCS) zu verwenden ist.

Benutzerbeschreibungsdaten

GROUP-IDENTIFICATION
Legt durch Angabe der Gruppenkennung die Benutzergruppe fest, der die Benutzerkennung zugeordnet ist.

PUBLIC-VOLUME-SET
Bestimmt den Pubset, dessen Benutzerkatalog den Eintrag der Benutzerkennung aufnimmt.

DEFAULT-PUBSET
Ordnet dem Benutzer einen Benutzer-Default-Pubset zu.

DEFAULT-MSG-SEARCH
Gibt an, in welchen Meldungsdateien Meldungstexte standardmäßig gesucht werden sollen.

DEFAULT-MSG-LANGUAGE
Gibt die Sprache an, in der standardmäßig die Meldungsausgabe erfolgen soll.

MAILING-ADDRESS
Legt die Versandanschrift für SPOOLOUT-Listen fest.

Zugangskontrolldaten

Die folgenden drei Zugangskontrolldaten können mit den Kommandos SET-LOGON-PROTECTION, MODIFY-LOGON-PROTECTION, ADD-USER und MODIFY-USER festgelegt werden.

LOGON-PASSWORD
Legt ein Kennwort für eine Benutzerkennung fest.

PASSWORD-ENCRYPTION
Legt fest, ob das unter LOGON-PASSWORD angegebene Kennwort verschlüsselt oder in Originalform gespeichert wird.

PASSWORD-MANAGEMENT
Vereinbart, ob der Benutzer sein Kennwort verändern bzw. löschen darf.

Die übrigen Zugangskontrolldaten können nur über die Kommandos SET-LOGON-PROTECTION bzw. MODIFY-LOGON-PROTECTION vereinbart werden:

PASSWORD
Legt weitere Attribute für die Verwendung von Kennwörtern fest, z.B.

- Minimale Länge des Kennworts (Operand MINIMAL-LENGTH),
- Minimale Komplexität des Kennworts (Operand MINIMAL-COMPLEXITY),
- Lebensdauer eines Kennworts (Operand LIFETIME).

EXPIRATION-DATE
Gibt das Datum an, nach der die Benutzerkennung gesperrt wird.

DIALOG-ACCESS
Definiert die im Dialogbetrieb wirksamen Zugangskontrollen, z.B. Einschränkung des Zugangs auf bestimmte Anschlußstellen (Operand TERMINALS-ALLOWED) oder den Schutz der Benutzerkennung durch die Chipkarte (Operand CHIPCARD).

BATCH-ACCESS
Definiert die im Stapelbetrieb wirksamen Zugangskontrollen, z.B. Einschränkung des Zugangs auf bestimmte Benutzerkennungen (Operand USER-ACCESS).

RBATCH-ACCESS
Legt fest, ob Fernstapelaufträge für eine Benutzerkennung zugelassen sind.

Rechte für Aufträge bzw. Tasks

Jedem Benutzerauftrag wird zu Beginn der Bearbeitung eine Task zugeordnet, die die Privilegien der Benutzerkennung übernimmt, die im LOGON-Kommando angegeben wurde. Zusätzliche Privilegien auf ablaufspezifische Objekte, wie Dateien, Jobvariable, Schalter etc. werden der Task bei ihrer Abarbeitung zugewiesen (siehe Seite 130).

Informationskommandos

Auskunft über Benutzerkennungen und Benutzergruppen erhält der Benutzer durch vier Informationskommandos. Alle Informationskommandos besitzen Operanden, die eine gezielte Auswahl der gewünschten Informationen bewirken (siehe Anhang A). Über welche Benutzerkennungen Informationen ausgegeben werden, hängt von der Ausstattung der Benutzerkennung ab, unter der eines dieser Kommandos abgesetzt wird. Dabei werden drei Gruppen von Kommandoaufrufern unterschieden:

- Benutzer, die keine Rechte bezüglich der Benutzerverwaltung und der Systemverwaltung besitzen.
- Benutzer, die das Gruppenverwalterrecht besitzen.
- Benutzer, die das Privileg USER-ADMINISTRATION besitzen.

SHOW-USER-ATTRIBUTES

Anzeigen von Benutzerrechten:

Kommandoaufrufer	Ausgabe
keine Rechte zur Benutzer- und Systemverwaltung	Benutzerrechte und Benutzerbeschreibungsdaten der eigenen Benutzerkennung
Gruppenverwalter-recht	Benutzerrechte und Benutzerbeschreibungsdaten aller Benutzerkennungen der eigenen und der untergeordneten Benutzergruppen
Privileg USER-ADMINISTRATION	Benutzerprivilegien und Benutzerbeschreibungsdaten aller Benutzerkennungen

Beispiel für einen privilegierten Aufrufer

```
/show-user-attributes user-identification=userid1,
information=*attributes(password-inf=summary),public-volume-set=*home,
output=sysout

SHOW-USER-ATTRIBUTES ── PVS A    - USER USERID1           1992-09-03 10:02:02
 ──────────────────────────────────────────────────────────────────────────
 USER-ID                     USERID1          PUBLIC-SPACE-USED              0
 GROUP-ID                 *UNIVERSAL          PUBLIC-SPACE-LIMIT      16777215
 DEFAULT-PUBSET                 A             PUBLIC-SPACE-EXCESS          *NO
 MAX-ACCOUNT-RECORDS          100             TEMP-SPACE-USED                0
 DEFAULT-MSG-LANGUAGE                         TEMP-SPACE-LIMIT       2147483647
                                              FILES                          0
 PROTECTION-ATTRIBUTES...                     FILE-NUMBER-LIMIT       16777215
 LOGON-PASSWORD               *YES            JOB-VARIABLES                  0
 PASSWORD-MGMT              *BY-USER          JV-NUMBER-LIMIT         16777215
 TAPE-ACCESS                  *STD            RESIDENT-PAGES             32767
 FILE-AUDIT                    *NO            ADDRESS-SPACE-LIMIT           16
                                              DMS-TUNING-RESOURCES        *NONE
 TEST-OPTIONS...                              CSTMP-MACRO-ALLOWED          *NO
 READ-PRIVILEGE                 1             CODED-CHARACTER-SET      EDF03IRV
 WRITE-PRIVILEGE                1
 MODIFICATION            *CONTROLLED          USER-LOCKED                  *NO

 PROFILE-ID  *NONE
 MAIL-ADDRESS  SECOS C/O SIEMENS NIXDORF INFORMATIONSSYSTEME GMBH GERMANY

 +──────────+────────────+──────────+─────────+──────────────+────────+──────+──────+
 !ACCOUNT-#! CPU-LIMIT !SPOOLOUT-!MAX-RUN-!MAX-ALLOWED-!NO-CPU-!START-!INHIB-!
 !          !           !  CLASS  !PRIORITY!  CATEGORY  ! LIMIT ! IMMED! DEACT!
 +──────────+────────────+──────────+─────────+──────────────+────────+──────+──────+
 ! X1234ABC!      65535!     0    !   255   !     STD     !   NO   !   NO !   NO !
 +──────────+────────────+──────────+─────────+──────────────+────────+──────+──────+

 DEFAULT-JOB-CLASS FOR BATCH-JOBS:  JC1B
 DEFAULT-JOB-CLASS FOR DIALOG-JOBS: JC1D
 LIST OF JOB-CLASSES ALLOWED:
 JC1B     JC1D
 ──────────────────────────────────────────────────────────────────────────
 SHOW-USER-ATTRIBUTES              END OF DISPLAY FOR USER USERID1  ON PVS A
```

SHOW-LOGON-PROTECTION

Anzeigen der Zugangskontrolldaten:

Kommandoaufrufer	Ausgabe
keine Rechte zur Benutzer- und Systemverwaltung	Zugangskontrolldaten der eigenen Benutzerkennung
Gruppenverwalter-recht	Zugangskontrolldaten aller Benutzerkennungen der eigenen und der untergeordneten Benutzergruppen
Privileg USER-ADMINISTRATION	Zugangskontrolldaten aller Benutzerkennungen

Beispiel für den privilegierten Benutzer

```
/show-logon-protection user-identification=userid1

  LOGON PROTECTION FOR USERID USERID1  ON PVS A
  EXPIRATION DATE:     NONE
  PASSWORD:            YES
      MANAGEMENT:      BY USER
      MINIMAL LENGTH:  NONE              MINIMAL COMPLEXITY:  NONE
      LIFETIME:        UNLIMITED
  DIALOG ACCESS:       YES               PASSWORD CHECK:      YES
      TERMINAL NAME:   ANY               CHIPCARD:            NO PROTECTION
  BATCH ACCESS:        YES               PASSWORD CHECK:      YES
      CALLER USERID:   ALL
  REMOTE BATCH ACCESS: YES               PASSWORD CHECK:      YES
  OPERATOR ACCESS TERM:YES               PASSWORD CHECK:      YES
      CHIPCARD:        NO PROTECTION
  OPERATOR ACCESS PROG:YES               PASSWORD CHECK:      YES
```

SHOW-USER-GROUP

Anzeigen von Informationen über Benutzergruppen und Gruppenmitglieder (Besitzt der Kommandoaufrufer keine Rechte bezüglich der Benutzer- und Systemverwaltung, so erhält er keine Informationen über Benutzergruppenstrukturen auf Daten-Pubsets):

Kommandoaufrufer	Ausgabe
keine Rechte zur Benutzer- und Systemverwaltung	Name der eigenen Benutzerkennung und Namen der Benutzerkennungen der eigenen Benutzergruppe
Gruppenverwalter-recht	Gruppenmitglieder, Gruppenpotential und Gruppenbeschreibungsdaten der eigenen und der untergeordneten Benutzergruppen
Privileg USER-ADMINISTRATION	Gruppenmitglieder, Gruppenpotential und Gruppenbeschreibungsdaten aller Benutzergruppen

Beispiel für den privilegierten Benutzer

```
/show-user-group group-identification=secos

SHOW-USER-GROUP   INFORMATION = *ALL                        1992-09-03 10:13:16

 GROUP-IDENTIFICATION            SECOS    PUBLIC-VOLUME-SET                   A
 GROUP-ADMINISTRATOR           USERID1    ADM-AUTHORITY          *MANAGE-MEMBERS
 USER-GROUP-PREFIX               *ANY     GROUP-MEMBER-PREFIX                SEC
 UPPER-GROUP                *UNIVERSAL

 MAX-SUB-GROUPS...
 LIMIT GROUP-HIERARCHY              0    LIMIT USER-ADM                       0
 FREE  GROUP-HIERARCHY              0    FREE  USER-ADM                       0
 MAX-GROUP-MEMBERS...
 LIMIT GROUP-HIERARCHY              0    LIMIT USER-ADM                       4
 FREE  GROUP-HIERARCHY              0    FREE  USER-ADM                       2

 TEST-OPTIONS...
 MODIFICATION               *CONTROLLED
 READ-PRIVILEGE                     1    WRITE-PRIVILEGE                      1

 PUBLIC-SPACE-EXCESS              *NO    PUBLIC-SPACE-LIMIT       2.147.483.647
 RESIDENT-PAGES                32.767    ADDRESS-SPACE-LIMIT                 16
 FILE-AUDIT                       *NO    CSTMP-MACRO                        *NO
 MAX-ACCOUNT-RECORDS              100    TAPE-ACCESS                      *STD
 TEMP-SPACE-LIMIT       2.147.483.647    DMS-TUNING-RESOURCES             *NONE
 FILE-NUMBER-LIMIT         16.777.215    JV-NUMBER-LIMIT             16.777.215

 NO PROFILE-ID SPECIFIED

 NO ACCOUNT-ATTRIBUTE SPECIFIED

 NO SUB-GROUP SPECIFIED

 GROUP-MEMBERS                SECID1    USERID1

SHOW-USER-GROUP   INFORMATION = *ALL                          END OF DISPLAY
```

SHOW-PRIVILEGE

Anzeigen von Privilegien (Dieses Kommando kann zwar von allen Benutzerkennungen abgesetzt werden, dient jedoch vor allem dem Sicherheitsbeauftragten, dem alle Benutzerkennungen mit den zugeteilten Privilegien angezeigt werden):

Kommandoaufrufer	Ausgabe
keine Rechte zur Benutzer- und Systemverwaltung	Es wird mitgeteilt, daß keine Systemverwalterrechte zugeteilt sind
Gruppenverwalterrecht	Es wird mitgeteilt, daß keine Systemverwalterprivilegien zugeteilt sind
Privileg USER-ADMINISTRATION	Es wird mitgeteilt, daß das Systemverwalterprivileg USER-ADMINISTRATION und evtl. weitere Systemverwalterprivilegien zugeteilt sind.

Beispiel

```
/show-privilege information=privilege(user-identification=userid1)

PRIVILEGES AVAILABLE TO USER-IDENTIFICATION USER1 ON PVS ABC1
PRIVILEGES:
STD-PROCESSING
PRIVILEGE SETS:
ARCHIV
```

5.2.2 Gruppenspezifische Benutzerverwaltung

Die gruppenspezifische Benutzerverwaltung wird von Gruppenverwaltern wahrgenommen. Gruppenverwalter sind Anwender im Teilnehmerbetrieb, denen durch einen Eintrag im Gruppenpotential das Gruppenverwalterrecht zugewiesen wurde. Ein Gruppenverwalter kann seine Funktion auf allen Pubsets erfüllen, auf denen er als Gruppenverwalter eingetragen ist. Es gibt drei Ausprägungen des Gruppenverwalterrechts, die zur Ausführung bestimmter Tätigkeiten berechtigen (siehe auch Bild 8):

MANAGE-RESOURCES

Dieses Recht berechtigt den Gruppenverwalter dazu, die Benutzerkennungen der eigenen und der untergeordneten Benutzergruppen sowie untergeordnete Benutzergruppen zu verwalten. Seine Tätigkeit ist auf bereits eingerichtete Benutzerkennungen und Benutzergruppen eingeschränkt.

MANAGE-MEMBERS

Dieses Recht berechtigt den Gruppenverwalter zusätzlich dazu, seine und untergeordnete Benutzergruppen durch Einrichten, Umhängen und Löschen von Gruppenmitgliedern zu verändern. Das MANAGE-MEMBERS-Recht schließt das MANAGE-RESOURCES-Recht ein.

MANAGE-GROUPS

Dieses Recht berechtigt den Gruppenverwalter zusätzlich dazu, die hierarchisch unter seiner Benutzergruppe liegende Gruppenstruktur durch Einrichten, Löschen und Umhängen von Untergruppen zu verändern. Das MANAGE-GROUPS-Recht schließt das MANAGE-MEMBERS-Recht ein.

Bei der Ausführung der Tätigkeiten, die den verschiedenen Ausprägungen des Gruppenverwalterrechts zugeordnet sind, ist folgendes zu beachten:

– Alle Tätigkeiten beziehen sich nur auf die eigene Benutzergruppe (bei der Verwaltung der Gruppenmitglieder) oder auf hierarchisch untergeordnete Benutzergruppen eines Pubset (bei der Verwaltung von Untergruppen und deren Gruppenmitgliedern), jedoch nie auf hierarchisch übergeordnete Benutzergruppen oder auf Benutzergruppen in anderen Pubsets.
– Die Ausprägung des Gruppenverwalterrechts kann nur bei der Verwaltung der entsprechenden Benutzergruppe festgelegt werden, und zwar durch einen hierarchisch übergeordneten Gruppenverwalter oder einen systemglobalen Benutzerverwalter.

Mit dem Kommando SHOW-USER-GROUP kann abgefragt werden, welche Ausprägung des Gruppenverwalterrechts vergeben wurde.

Im folgenden werden die Tätigkeiten, die ein Gruppenverwalter ausführen kann, entsprechend den Ausprägungen des Gruppenverwalterrechts näher beschrieben.

5.2.3 Gruppenverwaltung mit dem MANAGE-RESOURCES-Recht

Ein Gruppenverwalter mit dem MANAGE-RESOURCES-Recht kann folgende Tätigkeiten ausführen:

- Verwaltung von Benutzerkennungen,
- Verwaltung der Gruppenpotentiale und Festlegung der Gruppenbeschreibungsdaten von Benutzergruppen,
- Ernennen, Austauschen und Absetzen von Gruppenverwaltern,
- Informieren über Benutzerkennungen und Benutzergruppen.

Verwaltung von Benutzerkennungen

Die Verwaltung bereits existierender Benutzerkennungen in Abhängigkeit vom Gruppenpotential erfolgt mit dem Kommando MODIFY-USER. Es können Benutzerrechte vergeben und entzogen, sowie Benutzerbeschreibungsdaten verändert werden. Das MANAGE-RESOURCES-Recht erlaubt jedoch keine Änderung von Zugangskontrolldaten.

Benutzerrechte bezüglich der Abrechnungsnummer

ACCOUNT

Vergibt ein Gruppenverwalter eine Abrechnungsnummer an ein Gruppenmitglied, so wird geprüft, ob diese Nummer im Gruppenpotential enthalten ist. Abrechnungsnummern, die durch die systemglobale Benutzerverwaltung einem Gruppenmitglied zugeordnet wurden, können durch den Gruppenverwalter entzogen, nicht aber an andere Gruppenmitglieder vergeben werden.

MAX-ACCOUNT-RECORDS

Der Wert aus dem Gruppenpotential oder ein kleinerer Wert kann durch den Gruppenverwalter an ein Gruppenmitglied vergeben werden. Hat der Operand MAX-ACCOUNT-RECORDS im Gruppenpotential den Wert NO-LIMIT, so darf der Gruppenverwalter einen beliebigen Wert für Gruppenmitglieder vergeben.

CPU-LIMIT

Der Wert aus dem Gruppenpotential oder ein kleinerer Wert kann durch den Gruppenverwalter an ein Gruppenmitglied weitergegeben werden. Auch hier kann die systemglobale Benutzerverwaltung über das Gruppenpotential hinaus beliebige Zuteilungen vornehmen.

NO-CPU-LIMIT
START-IMMEDIATE
INHIBIT-DEACTIVATION

Für jedes dieser Benutzerrechte ist im Gruppenpotential ein Kennzeichen hinterlegt, das folgenden Wert annehmen kann:

YES: Der Gruppenverwalter kann dieses Benutzerrecht an Gruppenmitglieder vergeben.
NO: Der Gruppenverwalter kann dieses Benutzerrecht nicht an Gruppenmitglieder vergeben.

SPOOLOUT-CLASS

Werte 1-255, wobei der Wert 1 die höchste Priorität darstellt

MAXIMUM-RUN-PRIORITY

Werte 30-255, wobei der Wert 30 die höchste Priorität darstellt. Die Priorität aus dem Gruppenpotential oder eine geringere Priorität kann durch den Gruppenverwalter an ein Gruppenmitglied weitergegeben werden. Auch hier kann die systemglobale Benutzerverwaltung über das Gruppenpotential hinaus beliebige Zuteilungen vornehmen.

MAX-ALLOWED-CATEGORY

Welche Rechte der Gruppenverwalter einem Gruppenmitglied zuweisen kann, hängt davon ab, welcher Wert für diesen Operanden im Gruppenpotential hinterlegt ist. Ändert der Gruppenverwalter eine Benutzerkennung, wobei dem MAX-ALLOWED-CATEGORY-Operanden ein bestimmter Wert zugewiesen wird, so ist zu beachten:

Wert im Gruppenpotential	Wert im Kommando des Gruppenverwalters		
	STD	TP	SYS
STD	+	-	-
TP	+	+	-
SYS	-	+	+

\+ Kommando wird akzeptiert

\- Kommando wird abgewiesen

Pubset-spezifische Benutzerrechte

PUBLIC-SPACE-LIMIT, FILE-NUMBER-LIMIT, JV-NUMBER-LIMIT, TEMP-SPACE-LIMIT

Der Wert aus dem Gruppenpotential oder ein kleinerer Wert kann durch den Gruppenverwalter an ein Gruppenmitglied weitergegeben werden. Auch hier kann die systemglobale Benutzerverwaltung über das Gruppenpotential hinaus beliebige Zuteilungen vornehmen.

PUBLIC-SPACE-EXCESS

Für dieses Benutzerrecht ist im Gruppenpotential ein Kennzeichen hinterlegt, das folgenden Wert annehmen kann:

YES: Der Gruppenverwalter kann dieses Benutzerrecht an Gruppenmitglieder vergeben.
NO: Der Gruppenverwalter kann dieses Benutzerrecht nicht an Gruppenmitglieder vergeben.

Sonstige Benutzerrechte

TAPE-ACCESS

Welchen Wert der Gruppenverwalter einem Gruppenmitglied zuweisen kann, hängt davon ab, welcher Wert für diesen Operanden im Gruppenpotential hinterlegt ist. Ändert der Gruppenverwalter eine Benutzerkennung, wobei dem TAPE-ACCESS-Operanden ein bestimmter Wert zugewiesen wird, so ist zu beachten:

Wert im Gruppenpotential	Wert im Kommando des Gruppenverwalters				
	STD	PRIV	READ	BYPASS-LABEL	ALL
STD	+	-	-	-	-
PRIV	+	+	-	-	-
READ	+	-	+	-	-
BYPASS-LABEL	+	-	+	+	-
ALL	+	+	+	+	+

\+ Kommando wird akzeptiert
– Kommando wird abgewiesen

CSTMP-MACRO-ALLOWED
FILE-AUDIT

Für jedes dieser Benutzerrechte ist im Gruppenpotential ein Kennzeichen hinterlegt, das folgenden Wert annehmen kann:

YES: Der Gruppenverwalter kann dieses Benutzerrecht an Gruppenmitglieder vergeben.
NO: Der Gruppenverwalter kann dieses Benutzerrecht nicht an Gruppenmitglieder vergeben.

TEST-OPTIONS

Die im Gruppenpotential festgelegten Werte für die Testprivilegierungen (Operanden READ-PRIVILEGE und WRITE-PRIVILEGE) stellen die Maximalwerte dar, die der Gruppenverwalter an Gruppenmitglieder weiterreichen kann. Der im Gruppenpotential dem Operanden MODIFICATION zugewiesene Wert hat folgende Bedeutung:

CONTROLLED: Nur dieser Wert kann einem Gruppenmitglied zugewiesen werden
UNCONTROLLED: Sowohl der Wert CONTROLLED als auch der Wert UNCONTROLLED können einem Gruppenmitglied zugewiesen werden.

Empfehlung:

An Benutzerkennungen sollte READ-PRIVILEGE=1 und WRITE-PRIVILEGE=1 vergeben werden.

PROFILE-ID

Der Gruppenverwalter kann einem Gruppenmitglied nur solche Syntaxdateien zuordnen, die im Gruppenpotential vorhanden sind. Syntaxdateien, die durch die systemglobale Benutzerverwaltung einem Gruppenmitglied zugeordnet wurden, können durch den Gruppenverwalter entzogen, nicht aber an andere Gruppenmitglieder vergeben werden.

ADDRESS-SPACE-LIMIT
RESIDENT-PAGES

Der Wert aus dem Gruppenpotential oder ein kleinerer Wert kann durch den Gruppenverwalter an ein Gruppenmitglied weitergegeben werden. Auch hier kann die systemglobale Benutzerverwaltung über das Gruppenpotential hinaus beliebige Zuteilungen vornehmen.

Benutzerbeschreibungsdaten

DEFAULT-PUBSET
MAILING-ADDRESS
DEFAULT-MSG-LANGUAGE
DEFAULT-MSG-SEARCH

Diese Benutzerbeschreibungsdaten sind nicht an eine Benutzergruppe gebunden. Sie können vom Gruppenverwalter ohne Einschränkungen an Gruppenmitglieder vergeben werden.

GROUP-IDENTIFICATION

Die Gruppenkennung kann beim Kommando MODIFY-USER nicht angegeben werden. Die Zuordnung von Benutzerkennungen zu Benutzergruppen erfolgt mit den Kommandos ADD-USER, ADD-USER-GROUP bzw. MODIFY-USER-GROUP. Das Absetzen dieser Kommandos ist jedoch mit dem MANAGE-RESOURCES-Recht nicht möglich.

PUBLIC-VOLUME-SET

Gibt den Pubset an, dessen Benutzerkatalog die durch den Operanden USER-IDENTIFICATION spezifizierte Benutzerkennung enthält.

Verwaltung des Gruppenpotentials und Festlegung der Gruppenbeschreibungsdaten von Benutzergruppen

Das Gruppenpotential von Untergruppen kann beim Ändern von Untergruppen mit dem Kommando MODIFY-USER-GROUP versorgt werden.

Das Potential an Benutzerrechten, das ein Gruppenverwalter vergeben darf, kann in folgende Klassen eingeteilt werden:

Gruppenpotential an Benutzerrechten bezüglich der Abrechnungsnummer

ADD-ACCOUNT
MOD-ACCOUNT
REM-ACCOUNT

Vereinbart ein Gruppenpotential an Abrechnungsnummern, das der Gruppenverwalter Gruppenmitgliedern und Untergruppen zuordnen kann.

MAX-ACCOUNT-RECORDS

Legt das Gruppenpotential bezüglich der Vergabe der Rechte zum Sammeln benutzerspezifischer Abrechnungssätze fest.

CPU-LIMIT

Legt das Gruppenpotential an CPU-Sekunden fest, das maximal an Gruppenmitglieder und Untergruppen weitergegeben werden kann.

NO-CPU-LIMIT
START-IMMEDIATE
INHIBIT-DEACTIVATION

Für jedes dieser Benutzerrechte wird im Gruppenpotential ein Kennzeichen hinterlegt, das folgenden Wert annehmen kann:

YES: Der Gruppenverwalter kann dieses Benutzerrecht an Gruppenmitglieder und Untergruppen vergeben.
NO: Der Gruppenverwalter kann dieses Benutzerrecht nicht an Gruppenmitglieder und Untergruppen vergeben.

SPOOLOUT-CLASS

Legt die höchstmögliche Spoolout-Klasse fest, die an Gruppenmitglieder oder Untergruppen weitergegeben werden kann.

MAXIMUM-RUN-PRIORITY

Legt die maximale Priorität, die einer Task zu Bearbeitungsbeginn zugewiesen werden kann, als Gruppenpotential fest.

MAX-ALLOWED-CATEGORY

Legt fest, für die Benutzung welcher Kategorien (Stapel-, Dialog- oder Transaktionsaufträge) Gruppenmitglieder oder Untergruppen autorisiert werden können.

Gruppenpotential an pubset-spezifischen Benutzerrechten

PUBLIC-SPACE-LIMIT

Der Wert aus dem Gruppenpotential oder ein kleinerer Wert kann durch den Gruppenverwalter an ein Gruppenmitglied weitergegeben werden. Auch hier kann die systemglobale Benutzerverwaltung über das Gruppenpotential hinaus beliebige Zuteilungen vornehmen.

PUBLIC-SPACE-EXCESS

Für dieses Benutzerrecht ist im Gruppenpotential ein Kennzeichen hinterlegt, das folgenden Wert annehmen kann:

YES: Der Gruppenverwalter kann dieses Benutzerrecht an Gruppenmitglieder vergeben.
NO: Der Gruppenverwalter kann dieses Benutzerrecht nicht an Gruppenmitglieder vergeben.

Sonstige Benutzerrechte

PUBLIC-SPACE-LIMIT

Legt das Gruppenpotential an Speicherplatz fest, das maximal an die Untergruppen oder Gruppenmitglieder einer Benutzergruppe vergeben werden kann.

PUBLIC-SPACE-EXCESS

Für dieses Benutzerrecht wird im Gruppenpotential ein Kennzeichen hinterlegt, das folgenden Wert annehmen kann:

YES: Der Gruppenverwalter kann dieses Benutzerrecht an Gruppenmitglieder und Untergruppen vergeben.
NO: Der Gruppenverwalter kann dieses Benutzerrecht nicht an Gruppenmitglieder und Untergruppen vergeben.

Gruppenpotential an sonstigen Benutzerrechten

TAPE-ACCESS

Regelt die Verwaltungsrechte des Gruppenverwalters bezüglich der Behandlung von Magnetbändern.

FILE-AUDIT
CSTMP-MACRO-ALLOWED

Für jedes dieser Benutzerrechte wird im Gruppenpotential ein Kennzeichen hinterlegt, das folgenden Wert annehmen kann:

YES: Der Gruppenverwalter kann dieses Benutzerrecht an Gruppenmitglieder und Untergruppen vergeben.
NO: Der Gruppenverwalter kann dieses Benutzerrecht nicht an Gruppenmitglieder und Untergruppen vergeben.

TEST-OPTIONS

Legt die Berechtigung bezüglich der Vergabe der Testprivilegierung fest. Die vergebenen Werte regeln die Rechte des Gruppenverwalters bei der Administration der Gruppenmitglieder bzw. der Untergruppen. Neben den maximalen Testprivilegierungen wird im Operanden MODIFICATION festgehalten, ob der Gruppenverwalter nur den Wert CONTROLLED oder auch den Wert UNCONTROLLED an Gruppenmitglieder bzw. Untergruppen weiterreichen darf.

ADD-PROFILE-ID
REM-PROFILE-ID

Vereinbart ein Gruppenpotential an Einträgen in der SDF-Parameterdatei, die der Gruppenverwalter Gruppenmitgliedern und Untergruppen zuordnen kann.

ADDRESS-SPACE-LIMIT

Vereinbart den maximal verfügbaren Benutzeradreßraum.

RESIDENT-PAGES

Regelt die Berechtigung, residente Teile des Arbeitsspeichers zu verwenden.

Gruppenbeschreibungsdaten

MAX-GROUP-MEMBERS

Legt die maximale Anzahl der Gruppenmitglieder fest, die eine Benutzergruppe in dem durch den Operanden PUBLIC-VOLUME-SET spezifizierten Pubset besitzen darf. Die Begrenzung gilt für die Summe der Benutzerkennungen der im Kommando spezifizierten Benutzergruppe und der ihr hierarchisch untergeordneten Benutzergruppen.

MAX-SUB-GROUPS

Legt die maximale Anzahl von Untergruppen fest, die eine Benutzergruppe in dem durch den Operanden PUBLIC-VOLUME-SET spezifizierten Pubset besitzen darf. Die Begrenzung umfaßt die Summe der Benutzergruppen, die hierarchisch der im Kommando spezifizierten Benutzergruppe untergeordnet sind.

GROUP-ADMINISTRATOR

Vereinbart keinen oder einen Gruppenverwalter aus der Menge der Gruppenmitglieder einer Benutzergruppe.

ADM-AUTHORITY

Vereinbart, in welcher Ausprägung das Gruppenverwalterrecht an den Gruppenverwalter vergeben wird.

Ein systemglobaler Benutzerverwalter kann zusätzlich eine maximale Anzahl von Gruppenmitgliedern (MAX-GROUP-MEMBERS) und Untergruppen (MAX-SUB-GROUPS) vergeben. Über diese Potentiale können auch Gruppenverwalter verfügen; sie können diese Potentiale jedoch nicht verändern.

Ernennen, Austauschen und Absetzen von Gruppenverwaltern

Das Ernennen, Austauschen und Absetzen von Gruppenverwaltern erfolgt für eine bereits existierende Benutzerkennung mit dem Kommando MODIFY-USER-GROUP über den Operanden GROUP-ADMINISTRATOR. Beim Austauschen und Absetzen wird der ehemalige Gruppenverwalter ein normales Gruppenmitglied. Für eine Benutzergruppe darf höchstens ein Gruppenverwalter ernannt werden. Wird kein Gruppenverwalter ernannt, kann eine Benutzergruppe von einem hierarchisch übergeordneten Gruppenverwalter und von allen systemglobalen Benutzerverwaltern verwaltet werden.

Informieren über Benutzerkennungen und Benutzergruppen

Mit den Kommandos SHOW-USER-ATTRIBUTES, SHOW-LOGON-PROTECTION und SHOW-USER-GROUP können Informationen über die einzelnen Benutzerkennungen und Benutzergruppen der untergeordneten Gruppenhierarchie ausgegeben werden (siehe "Informationskommandos", Seite 63).

5.2.4 Gruppenverwaltung mit dem MANAGE-MEMBERS-Recht

Ein Gruppenverwalter mit dem MANAGE-MEMBERS-Recht kann folgende Tätigkeiten ausführen:

- alle Tätigkeiten, die ein Gruppenverwalter mit dem MANAGE-RESOURCES-Recht ausführen kann,
- Einrichten von Benutzerkennungen,
- Löschen von Benutzerkennungen,
- Sperren bzw. Freigeben von Benutzerkennungen,
- Umhängen von Benutzerkennungen,
- Festlegung von Zugangskontrolldaten für Benutzerkennungen.

Einrichten von Benutzerkennungen

Benutzerkennungen werden mit dem Kommando ADD-USER eingerichtet und können durch Angabe der Gruppenkennung in eine Benutzergruppe eingehängt werden (Operand GROUP-IDENTIFICATION). Das Kommando wird abgewiesen, wenn die maximale Anzahl von Gruppenmitgliedern überschritten wird oder wenn ein Benutzerrecht vergeben wird, das im Gruppenpotential nicht enthalten ist.

Löschen von Benutzerkennungen

Das Löschen von Benutzerkennungen erfolgt mit dem Kommando REMOVE-USER.

Sperren bzw. Freigeben von Benutzerkennungen

Mit dem Kommando LOCK-USER bzw. über den Operanden LOCK des Kommandos ADD-USER wird eine Benutzerkennung sofort gesperrt. Für eine gesperrte Benutzerkennung ist bis zu ihrer expliziten Freigabe kein Zugang zum BS2000 möglich. Benutzerkennungen mit laufenden Aufträgen können bis zum Auftragsende nicht gesperrt werden.

Das Sperren einer Benutzerkennung kann sinnvoll sein, um andere, die Benutzerkennung betreffende Kommandos abzusetzen, ohne ein LOGON-Kommando auf die Benutzerkennung zuzulassen. Die Freigabe der Benutzerkennung geschieht explizit durch das Kommando UNLOCK-USER.

Umhängen von Benutzerkennungen

Innerhalb einer Gruppenstruktur kann eine Benutzerkennung mit dem Kommando MODIFY-USER-GROUP von einer Benutzergruppe in eine andere umgehängt werden (Operand ADD-GROUP-MEMBER). Voraussetzung ist, daß beide Benutzergruppen der Gruppenstruktur, die dem Gruppenverwalter untergeordnet ist, angehören.

Beim Umhängen einer Benutzerkennung ist zu beachten, daß die Benutzerkennung nicht mit mehr Benutzerrechten ausgestattet sein darf, als aufgrund des Gruppenpotentials der neuen Benutzergruppe zulässig ist. Gegebenenfalls müssen vor dem Umhängen Anpassungen an die möglichen Rechte der neuen Benutzergruppe vorgenommen werden.

Festlegung von Zugangskontrolldaten für Benutzerkennungen

Alle Zugangskontrolldaten können mit den Kommandos SET-LOGON-PROTECTION bzw. MODIFY-LOGON-PROTECTION vereinbart und geändert werden. Überdies ermöglichen die Kommandos ADD-USER und MODIFY-USER die Angabe der Attribute LOGON-PASSWORD, PASSWORD-ENCRYPTION und PASSWORD-MANAGEMENT. Bei den Zugangskontrolldaten gibt es keine Einschränkungen durch das Gruppenpotential.

5.2.5 Gruppenverwaltung mit dem MANAGE-GROUPS-Recht

Ein Gruppenverwalter mit dem MANAGE-GROUPS-Recht kann folgende Tätigkeiten ausführen:

- alle Tätigkeiten, die ein Gruppenverwalter mit dem MANAGE-MEMBERS-Recht ausführen kann,
- Einrichten von Benutzergruppen,
- Löschen von Benutzergruppen,
- Umhängen von Benutzergruppen.

Einrichten von Benutzergruppen

Eine Benutzergruppe wird mit dem Kommando ADD-USER-GROUP eingerichtet. Über den Operanden GROUP-IDENTIFICATION erhält die Benutzergruppe eine eindeutige Gruppenkennung. Über den Operanden UPPER-GROUP wird gesteuert, an welche Benutzergruppe die neu zu erzeugende Benutzergruppe angehängt wird. Gleichzeitig können beim Einrichten einer Benutzergruppe über den Operanden ADD-GROUP-MEMBER Gruppenmitglieder zugeordnet werden. Diese müssen bereits vorhanden sein und dürfen der Benutzergruppe des Kommandoaufrufers hierarchisch nicht übergeordnet sein. Über den Operanden GROUP-ADMINISTRATOR kann ein Gruppenverwalter ernannt werden.

Die maximale Anzahl von Gruppenmitgliedern und die maximale Anzahl von Untergruppen werden mit dem Gruppenpotential der direkt übergeordneten Benutzergruppe verrechnet. Dabei kann auch das Gruppenpotential verwendet werden, das von einem systemglobalen Benutzerverwalter zugeordnet wurde.

Löschen von Benutzergruppen

Eine Benutzergruppe wird mit dem Kommando REMOVE-USER-GROUP gelöscht. Dazu darf sie keine Gruppenmitglieder und keine Untergruppen mehr besitzen. Diese müssen vorher explizit gelöscht oder in eine andere Benutzergruppe umgehängt worden sein. Die maximale Anzahl von Gruppenmitgliedern und die maximale Anzahl von Untergruppen werden dem Gruppenpotential der direkt übergeordneten Benutzergruppe zugewiesen, sofern es von einem Gruppenverwalter vergeben wurde. Das von einem systemglobalen Benutzerverwalter zugewiesene Gruppenpotential wird keiner Benutzergruppe zugerechnet.

Umhängen von Benutzergruppen

Es können Benutzergruppen mit dem Kommando MODIFY-USER-GROUP vollständig in eine andere Benutzergruppe der gleichen Gruppenstruktur umgehängt werden (Operand UPPER-GROUP). Voraussetzung hierfür ist, daß die abzuhängende Benutzergruppe eine dem Kommandoaufrufer untergeordnete Benutzergruppe ist und die Benutzergruppe, an die angehängt werden soll, die eigene oder eine untergeordnete Benutzergruppe des Kommandoaufrufers ist.

Bezüglich des Gruppenpotentials, der maximalen Anzahl von Gruppenmitgliedern und der maximalen Anzahl von Untergruppen ist zu beachten:

- Das Gruppenpotential der umzuhängenden Benutzergruppe, das von einem Gruppenverwalter vergeben wurde, wird der vor dem Umhängen direkt übergeordneten Benutzergruppe zugewiesen.
- Das Gruppenpotential der umzuhängenden Benutzergruppe, das von einem Gruppenverwalter vergeben wurde, darf nicht größer sein als das freie Gruppenpotential der neuen, direkt übergeordeten Benutzergruppe. Gegebenenfalls müssen vor dem Umhängen Anpassungen an die möglichen Rechte der neuen Benutzergruppe vorgenommen werden.
- Das von einem systemglobalen Benutzerverwalter zugewiesene Gruppenpotential verbleibt bei der umzuhängenden Benutzergruppe.

5.2.6 Benutzerverwaltung in einem MPVS-System

Ein Multiple-Public-Volume-Set-System (MPVS-System) besteht aus einer Anzahl von unterschiedlichen, unabhängigen Pubsets. Der Home-Pubset ist der Pubset, von dem die laufende BS2000-Sitzung gestartet wurde. Die übrigen Pubsets, die nur der Speicherung von Daten dienen, bezeichnet man als Daten-Pubsets. In jedem Pubset kann von der Benutzerverwaltung eine eigene Gruppenstruktur aufgebaut werden, die sich von Pubset zu Pubset unterscheiden kann. Das Gruppenverwalterrecht bezieht sich stets nur auf eine Gruppenstruktur eines Pubset. Die Systemverwalterrechte sind jedoch in allen Gruppenstrukturen gültig.

Überprüfung von Benutzerkennungen

Alle Benutzerkennungen, die Zugang zum Betriebssystem erhalten wollen, müssen einen Eintrag im Benutzerkatalog des Home-Pubset besitzen, sie können Einträge in den Benutzerkatalogen der Daten-Pubsets besitzen. Die Einträge einer Benutzerkennung in unterschiedlichen Pubsets müssen nicht identisch sein. Durch eine Generierungsoption kann festgelegt werden, ob bei einem Zugriff einer Benutzerkennung auf einen Daten-Pubset ein Eintrag der Benutzerkennung im Benutzerkatalog des Daten-Pubset erforderlich ist oder nicht.

Das BS2000 überprüft vor der Belegung von Speicherplatz auf einem Daten-Pubset auch die pubset-spezifischen Benutzerrechte PUBLIC-SPACE-LIMIT und evtl. PUBLIC-SPACE-EXCESS. Ist entsprechend der Generierungsoption ein Eintrag der Benutzerkennung im Benutzerkatalog des Daten-Pubset erforderlich, entnimmt das BS2000 diese beiden Benutzerrechte dem Benutzerkatalog des entsprechenden Daten-Pubset, die anderen Benutzerrechte dem Benutzerkatalog des Home-Pubset. Bei allen anderen Benutzeraktivitäten entnimmt das BS2000 die Benutzerrechte ausschließlich dem Benutzerkatalog des Home-Pubset.

Aus diesem Grund kann beim Eintragen einer Benutzerkennung in den Benutzerkatalog eines Daten-Pubset die Angabe der übrigen Benutzerrechte entfallen. Lediglich die pubset-spezifischen Benutzerrechte müssen angegeben werden, wenn sie einen Wert ungleich des Standardwerts erhalten sollen.

Beispiel 1: Eintragen der Benutzerkennung hannibal in den Benutzerkatalog des Home-Pubset

```
add-user user-identification=hannibal,tape-access=read,
group-identification=*own,public-space-limit=0,
public-volume-set=*std,default-pubset=a,account=12345678,
cpu-limit=20000,privilege=start-immediate
```

Beispiel 2: Eintragen der Benutzerkennung hannibal in den Benutzerkatalog des Daten-Pubset mit der Katalogkennung A

```
add-user user-identification=hannibal,
group-identification=*own,
public-space-limit=10000,
public-volume-set=a
```

Überprüfung von Benutzergruppen

Die Überprüfung des Gruppenpotentials einer Benutzergruppe erfolgt dagegen stets innerhalb eines Pubset. Das BS2000 unterscheidet dabei nicht, ob die Benutzergruppe auf dem Home-Pubset oder einem Daten-Pubset eingerichtet ist. Der Pubset wird durch den Operanden PUBLIC-VOLUME-SET der entsprechenden Kommandos (ADD-USER, ADD-USER-GROUP etc.) spezifiziert.

Es liegt im Verantwortungsbereich der Benutzerverwaltung auf den Pubsets effiziente Benutzergruppenstrukturen zu erzeugen. So ist es z.B. sinnvoll, auf dem Home-Pubset keinen gemeinschaftlichen Speicherplatz bezüglich der pubset-spezifischen Attribute an Benutzerkennungen und Benutzergruppen zu vergeben.

Wichtig:

- Soll der Zugriffsschutz über Benutzergruppen geregelt werden, so muß die entsprechende Benutzergruppenstruktur auf dem Home-Pubset aufgebaut sein.
- Benutzergruppenstrukturen auf Daten-Pubsets dienen einzig der Verwaltung pubset-spezifischer Attribute.

5.2.7 Systemglobale Benutzerverwaltung

Die systemglobale Benutzerverwaltung kann von allen Benutzerkennungen durchgeführt werden, denen vom Sicherheitsbeauftragten das Privilieg USER-ADMINISTRATION zugewiesen wurde. Diese Benutzerkennungen, die im folgenden als systemglobale Benutzerverwalter bezeichnet werden, können ihre Funktion jedoch nur erfüllen, wenn sie dieses Privileg auf dem Home-Pubset der laufenden BS2000-Sitzung besitzen.

Ein systemglobaler Benutzerverwalter kann insbesondere alle Benutzerkennungen und Benutzergruppen verwalten und ihnen über die bestehenden Gruppenpotentiale hinaus Benutzerrechte zuweisen. Er kann an beliebiger Stelle innerhalb einer Benutzergruppenstruktur

- Benutzerkennungen und Benutzergruppen einrichten, löschen, innerhalb einer Gruppenstruktur umhängen etc.,
- Gruppenverwalter ernennen, austauschen oder absetzen,
- Benutzerrechte an alle Benutzerkennungen und Benutzergruppen zuteilen oder entziehen. Diese Benutzerrechte werden nicht mit dem Gruppenpotential verrechnet. Sie gelten der Benutzerkennung bzw. der Benutzergruppe zugeordnet.

Für weiterführende Informationen wird auf das Sicherheitshandbuch für die Systemverwaltung [12] verwiesen.

5.2.8 Beispiele zur gruppenspezifischen Benutzerverwaltung

Die folgenden Beispiele beziehen sich auf die Gruppenstruktur in Bild 9:

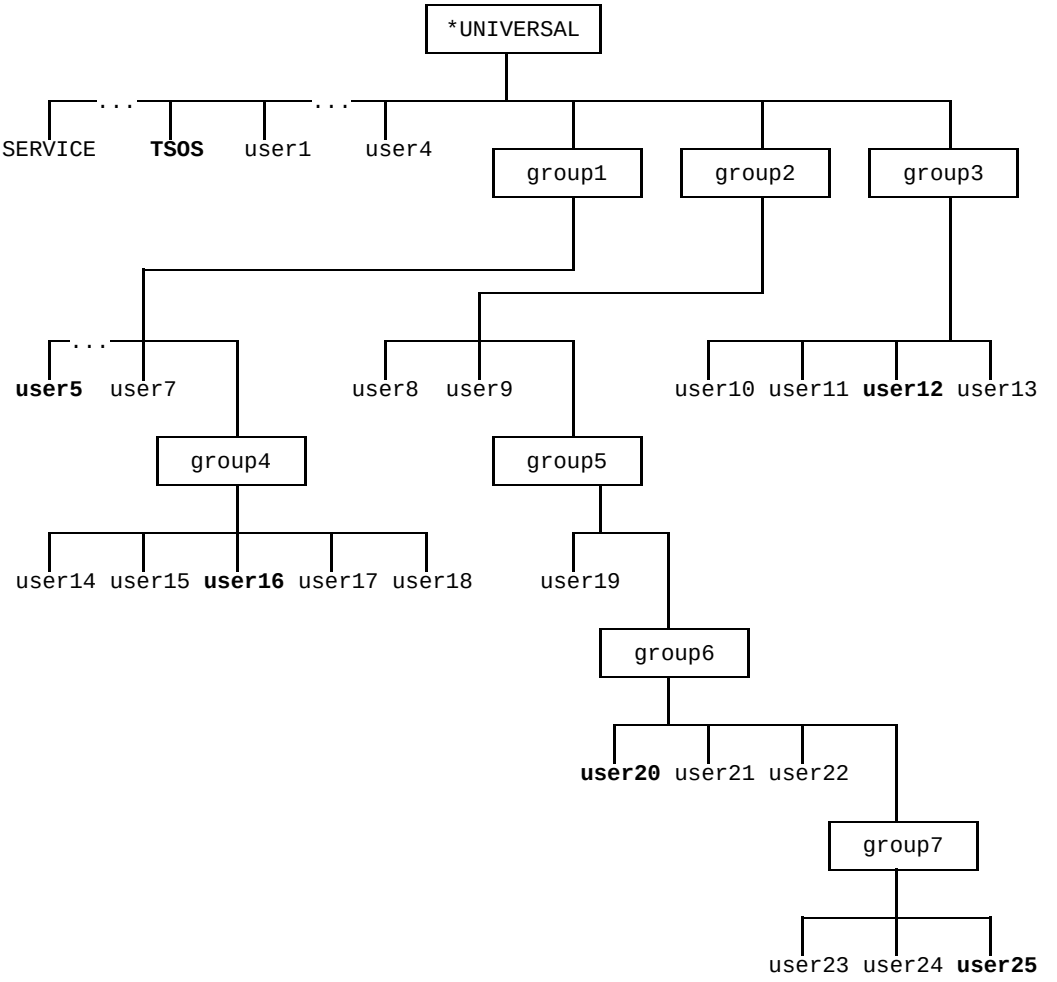


Bild 9: Gruppenstruktur vor den Modifikationen durch Beispiel 1 und Beispiel 2

Beispiel 1: Verwaltung bestehender Benutzergruppen

a) In die Benutzergruppe group2 soll eine Benutzerkennung user26 als Gruppenverwalter mit dem MANAGE-GROUPS-Recht eingerichtet werden.
b) Die Benutzergruppe group7 soll aufgelöst werden.
c) Die Benutzergruppe group6 soll an die Benutzergruppe group2 umgehängt werden.

zu (a):

Da die Benutzergruppe group2 keinen übergeordneten Gruppenverwalter besitzt, muß der systemglobale Benutzerverwalter diese Aufgabe übernehmen:

```
add-user user-identification=user26,group-identification=group2

modify-user-group group-identification=group2,
                  group-administrator=user26,
                  adm-authority=manage-groups
```

zu (b):

Da der Gruppenverwalter user26 der Benutzergruppe group2 das MANAGE-GROUPS-Recht und somit auch das MANAGE-MEMBERS-Recht hat, kann er die Mitglieder der Benutzergruppe group7 und die Benutzergruppe group7 selbst löschen:

```
remove-user user-identification=user23
remove-user user-identification=user24
modify-user-group group-id=group7,group-adm=*none          *)
remove-user user-identification=user25

remove-user-group group-identification=group7
```

*) Das user25 Gruppenverwalter ist, kann die Kennung erst gelöscht werden, wenn die Kennung als Gruppenverwalter abgesetzt ist.

zu (c):

Der Gruppenverwalter mit der Benutzerkennung user26 verfügt auf Grund des MANAGE-GROUPS-Recht und der Gruppenhierarchie über die Berechtigung, die Benutzergruppe group6 an die Benutzergruppe group2 anzuhängen.

```
modify-user-group group-identification=group6,upper-group=group2
```

Beispiel 2: Einrichten einer neuen Untergruppe

Für die Benutzergruppe group3 soll eine neue Untergruppe eingerichtet werden, die u.a. folgendes Gruppenpotential erhalten soll:

a) Die Gruppenkennung der neuen Untergruppe sei group8.
b) Gruppenmitglieder der Benutzergruppe group8 seien die Benutzerkennungen user10 und user11.
c) Gruppenverwalter der Benutzergruppe group8 sei die Benutzerkennung user10 mit der Berechtigung MANAGE-MEMBERS.
d) Maximal 6 Gruppenmitglieder sollen der Benutzergruppe group8 angehören dürfen.
e) Die Benutzergruppe group8 darf keine weiteren Untergruppen enthalten.
f) Als Abrechnungsnummer soll die Abrechnungsnummer 12345678 der Benutzergruppe group3 vergeben werden, mit den folgenden Parametereinstellungen: CPU-LIMIT=9999999 und PRIVILEGE=NO.
g) Für die Bandbehandlung betrage der Parameter TAPE-ACCESS=READ.
h) Der Parameter PUBLIC-SPACE-LIMIT soll den Wert 5000 PAM-Seiten erhalten.

Das Gruppenpotential der Benutzergruppe group3 kann über das Kommando SHOW-USER-GROUP abgefragt werden. Für die Benutzergruppe group3 ist u.a. folgendes Gruppenpotential vorhanden:

	Benutzergruppe: group3
GROUP-ADMINISTRATOR	user12
ADM-AUTHORITY	MANAGE-GROUPS
MAX-GROUP-MEMBERS	12
MAX-SUB-GROUPS	3
ACCOUNT	ACCOUNT-NUMBER = 12345678 CPU-LIMIT = MAXIMUM PRIVILEGE = NO-CPU-LIMIT ACCOUNT-NUMBER = 45678901 CPU-LIMIT = 9999999 PRIVILEGE = NO-CPU-LIMIT
PUBLIC-SPACE-LIMIT	20000
TAPE-ACCESS	READ

An die Gruppenmitglieder user10, user11, user12 und user13 seien u.a. folgende Benutzerrechte vergeben:

	Gruppenmitglieder			
	user10	user11	user12	user13
ACCOUNT ACCOUNT-NUMBER CPU-LIMIT PRIVILEGE ACCOUNT-NUMBER CPU-LIMIT PRIVILEGE ACCOUNT-NUMBER CPU-LIMIT PRIVILEGE	 12345678 MAXIMUM NO-CPU-LIMIT 45678901 MAXIMUM NO-CPU-LIMIT 78901234 (*) MAXIMUM NO-CPU-LIMIT	 12345678 MAXIMUM NO-CPU-LIMIT 45678901 MAXIMUM NO-CPU-LIMIT	 45678901 MAXIMUM NO-CPU-LIMIT	 12345678 MAXIMUM NO
PUBLIC-SPACE-LIMIT	1000	2000	1000	500
TAPE-ACCESS	STD	STD	READ	STD

(*) Diese Abrechnungsnummer wurde vom systemglobalen Benutzerverwalter vergeben. Sie ist daher nicht im Gruppenpotential vorhanden.

Die Benutzergruppe group3 besitzt 4 Gruppenmitglieder (user10, user11, user12, user13). Der Gruppenverwalter kann also noch bis zu 8 weitere Gruppenmitglieder einrichten (Wert für MAX-GROUP-MEMBERS - 4 = 8) bzw. noch maximal 3 Untergruppen (MAX-SUB-GROUPS=3).

Da die Benutzerkennungen user10 und user11 in der Benutzergruppe group3 über mehr Benutzerrechte verfügen, als ihnen entsprechend dem Gruppenpotential der neu einzurichtenden Untergruppe group8 zugeteilt werden kann, sind zunächst Anpassungen vorzunehmen. Der Gruppenverwalter user12 der Benutzergruppe group3 muß vor dem Einrichten der Untergruppe die Benutzerrechte der Benutzerkennungen user10 und user11 modifizieren. Andernfalls würden spätere Kommandos zum Umhängen von user10 und user11 in die neue Untergruppe abgewiesen. Die Benutzerkennungen user10 und user11 werden für die Dauer der Änderungen gesperrt, um den Zugang während der Kommandoeingaben zu unterbinden:

```
lock-user user-identification=user10
lock-user user-identification=user11

modify-user user-identification=user10,-
            account-attributes=remove(account=45678901,78901234),-
            account-attributes=modify(account=12345678,-
                                      cpu-limit=9999999,privilege=no)

modify-user user-identification=user11,-
            account-attributes=remove(account=45678901),-
            account-attributes=modify(account=12345678,-
                                     cpu-limit=9999999,privilege=no)
```

Danach kann die Untergruppe group8 mit den Gruppenmitgliedern user10 und user11 eingerichtet werden:

```
add-user-group group-identification=group8,-
               add-group-member=(user10,user11),-
               group-administrator=user10,-
               adm-authority=manage-members,-
               max-group-members=6,-
               max-sub-groups=0,-
               add-account=(12345678,(cpu-limit=9999999,privilege=no)),-
               tape-access=read,-
               public-space-limit=5000
```

Nach Abschluß der Änderungen können die Benutzerkennungen user10 und user11 wieder freigegeben werden:

```
unlock-user user-identification=user10
unlock-user user-identification=user11
```

Die neu eingerichtete Untergruppe group8 hat damit u.a. folgendes Gruppenpotential erhalten:

	Benutzergruppe: group8
GROUP-ADMINISTRATOR	user10
ADM-AUTHORITY	MANAGE-MEMBERS
MAX-GROUP-MEMBERS	6
MAX-SUB-GROUPS	0
ACCOUNT	ACCOUNT-NUMBER = 12345678 CPU-LIMIT = 9999999 PRIVILEGE = NO
PUBLIC-SPACE-LIMIT	50000
TAPE-ACCESS	READ

Die Gruppenmitglieder user10 und user11 verfügen u.a. über folgende Benutzerrechte:

	Gruppenmitglieder	
	user10	user11
ACCOUNT ACCOUNT-NUMBER CPU-LIMIT PRIVILEGE	 12345678 9999999 NO	 12345678 9999999 NO
PUBLIC-SPACE-LIMIT	1000	2000
TAPE-ACCESS	STD	STD

Die Benutzergruppe group3 besitzt nun 2 Gruppenmitglieder (user12, user13) und eine Untergruppe (group8) mit maximal 6 Gruppenmitgliedern, von denen ebenfalls 2 (user10, user11) eingerichtet sind. Der Gruppenverwalter von group3 kann demzufolge noch bis zu 4 weitere Gruppenmitglieder einrichten (Wert für MAX-GROUP-MEMBERS - 2 - 6 = 4) bzw. noch maximal 2 Untergruppen (Wert für MAX-SUB-GROUPS - 1 = 2). Die entsprechenden Werte für den Gruppenverwalter von group8 betragen 4 (Wert für MAX-GROUP-MEMBERS - 2 = 4) und 0 (Wert für MAX-SUB-GROUPS=0)

Aus den Beispielen 1 und 2 ergibt sich folgende neue Gruppenstruktur:

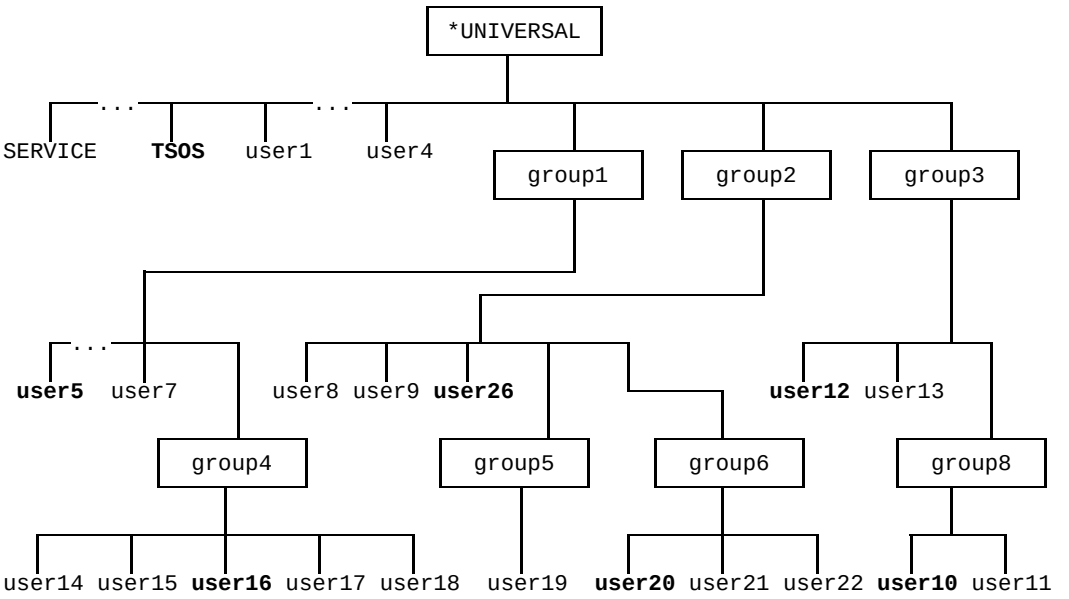


Bild 10: Gruppenstruktur nach den Modifikationen durch Beispiel 1 und Beispiel 2

6 Zugriffsschutz des BS2000

Zugriffsschutzmechanismen dienen dem Schutz vor unberechtigtem Zugriff auf gespeicherte Informationen. Im BS2000 wird der Zugriffsschutz durch eine Reihe aufeinander aufbauender Mechanismen realisiert. Diese beginnen bei der Gestaltung der Hardware-Software-Schnittstelle und reichen bis in die logisch höheren Schichten des Betriebssystems.

Das vorliegende Kapitel gibt zunächst einen Überblick über den hardware-unterstützten Zugriffsschutz des BS2000. Auf dieser Grundlage werden die Konzepte des Zugriffsschutzes vorgestellt. Anschließend wird der Zugriffsschutz für Dateien und weitere relevante Objekte des BS2000 erläutert. Empfehlungen zu organisatorischen Maßnahmen zur Unterstützung des Zugriffsschutzes finden sich am Ende des Kapitels.

6.1 Hardware-unterstützter Zugriffsschutz

Die Basis für die logisch höheren Ebenen des Zugriffsschutzes des BS2000 bilden Schutzmechanismen, die von der Hardware in Verbindung mit dem Betriebssystemkern bereitgestellt werden. Ihre wichtigste Aufgabe ist die Abschottung des Betriebssystems vom Benutzer.

Das BS2000 bietet drei Arten von hardware-unterstütztem Zugriffsschutz:

- Befehlsprivilegierung,
- virtuelle Adressierung und
- Speicherschutz.

6.1.1 Befehlsprivilegierung

Im Zusammenhang mit der Hardware-Software-Schnittstelle wird unter Befehlsprivilegierung ein Schutzmechanismus verstanden, der es gestattet, bestimmte Befehle nur in einem privilegierten Zustand des Zentralprozessors auszuführen. Durch Befehlsprivilegierung wird sichergestellt, daß der Zugriff auf Funktionen zur Steuerung der Hardware oder auf benutzerübergreifende Funktionen der Hardware-Software-Schnittstelle nur auf das Betriebssystem eingeschränkt ist.

6.1.2 Virtuelle Adressierung

Im BS2000 steht jeder Task ein eigener virtueller Adreßraum zur Verfügung. Ein virtueller Adreßraum ist ein zusammenhängender Adreßbereich, der byteweise fortlaufend durchnummeriert ist. Die adreßraumspezifische Adressierung beginnt bei 0 und kann bis zum theoretischen Maximum von 2 GByte reichen. Verwaltet wird ein virtueller Adreßraum in Einheiten von Segment und Seite, die jeweils eine feste Länge besitzen. Bei der Speicherzuteilung an eine Task wird eine Seite ihres virtuellen Adreßraums in einen gleichgroßen Seitenrahmen des Arbeitsspeichers übertragen. Die Abbildung von virtuellen Adressen auf reale Arbeitsspeicheradressen erfolgt durch einen Hardware-Mechanismus mit Hilfe von Adreßumsetzungstabellen.

Die Gesamtheit der virtuellen Adreßräume bildet den virtuellen Speicher des BS2000. Die gemeinsamen Adreßraumanteile werden als Systemadreßraum, die disjunkten taskspezifischen Adreßraumanteile als Benutzeradreßraum bezeichnet (siehe Bild 10).

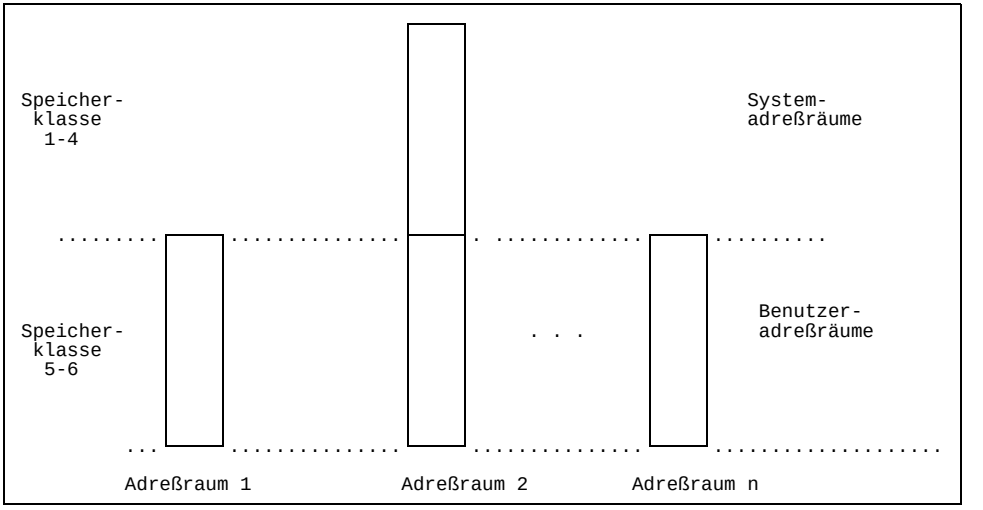


Bild 11: Adreßraumstruktur

Für die Zuteilung und Freigabe von Speicherbereichen ist der Adreßraum in 6 Speicherklassen unterteilt. Die Speicherklassen haben bestimmte Eigenschaften, die für alle in ihnen enthaltenen Seiten Gültigkeit besitzen (siehe Bild 12). Jede Seite ist eindeutig einer Speicherklasse zugeordnet. Der Systemadreßraum umfaßt die Speicherklassen 1 bis 4, der Benutzeradreßraum die Speicherklassen 5 und 6.

Klasse	Attribute	für	Inhalt
1	resident, statisch, privilegiert	Betriebssystem	residentes Systemprogramm, zentrale Systemtabellen
2	seitenwechselbar, statisch privilegiert	Betriebssystem	seitenwechselbare Systemprogramme
3	resident, dynamisch, privilegiert	Betriebssystem	residente Systemarbeitsbereiche residente Systemarbeitstabellen
4	seitenwechselbar dynamisch, privilegiert	Betriebssystem,	seitenwechselbare Systemarbeitsbereiche und -tabellen ablaufinvariante Programmsysteme (shared code)
5	seitenwechselbar dynamisch, privilegiert/ nicht privilegiert	Betriebssystem, Benutzer	Verbindungsbereich Betriebssystem/Benutzer
6	seitenwechselbar dynamisch, nicht privilegiert	Benutzer	Benutzerprogramme

Bild 12: Speicherklassen

Durch die virtuelle Adressierung wird gewährleistet, daß Programme verschiedener Benutzer in unterschiedlichen Adreßräumen ablaufen. Jeder Adreßraum ist vor Zugriffen durch Benutzerprogramme aus anderen Adreßräumen geschützt. Dieser Schutz wird durch die Adreßumsetzung sichergestellt, die sich - hardware-gesteuert - immer auf den Adreßraum bezieht, der bei der Initiierung einer Task eingeschaltet wurde. Task-Wechsel und Adreßraumwechsel sind so fest aneinander gekoppelt.

Das Betriebssystem bzw. der Benutzer kann Adreßraum als gemeinsam benutzbar zur Verfügung stellen (z.B. MEMORY Pools). Eine Sonderstellung nimmt der Systemadreßraum ein, in dem die Programme und Daten des Betriebssystems enthalten sind. Um zu ermöglichen, daß die Systemfunktionen von jedem Adreßraum aus ansprechbar sind, ist dieser Anteil mehrfach benutzbar.

6.1.3 Speicherschutz

Zum Schutz der Zugriffe auf den realen Arbeitsspeicher existiert seitenbezogen ein Schutzmechanismus, der nach dem Schloß-Schlüssel-Prinzip arbeitet. Der Schutz der Speicherbereiche ist realisiert durch ein Speicherschloß, das jeder Seite im Arbeitsspeicher zugeordnet ist, und einen Ablaufschlüssel für Programmläufe, der vom Betriebssystem eingestellt wird. Nur privilegierte Subsysteme des BS2000 setzen Speicherschlösser und Ablaufschlüssel.

Systemadreßraum und Benutzeradreßraum sind durch Speicherschutz voneinander abgeschottet. Die im Systemadreßraum ablaufenden Subsysteme des BS2000 sind privilegiert (Funktionsbereich TPR) und können auf den gesamten Adreßraum zugreifen. Die im Benutzeradreßraum ablaufenden Benutzerprogramme sind im allgemeinen nicht-privilegiert (Funktionsbereich TU); sie können nur auf den jeweiligen task-spezifischen Adreßraum zugreifen. Dabei ist sichergestellt, daß nicht-privilegiert ablaufende Programme immer mit nicht-privilegierten Schlüsseln ablaufen, so daß sie auf die vom BS2000 benutzten privilegierten Speicherseiten nicht zugreifen können. Die privilegiert ablaufenden Subsysteme des BS2000 sind so vor Fehlverhalten der Benutzerprogramme geschützt.

6.1.4 Wechsel der Funktionsbereiche

Der zentrale Mechanismus des BS2000 für den Aufruf von Funktionen des Betriebssystems durch Benutzerprogramme ist der Aufruf durch SVC (Supervisor Call). Dieser nicht-privilegierte Befehl bewirkt einen Wechsel des Funktionsbereichs der aufrufenden Task in den Funktionsbereich TPR. Bei Beendigung des Aufrufs wird wieder der nicht-privilegierte Funktionsbereich TU eingeschaltet.

6.2 Objektschutz des BS2000

Der Objektschutz des BS2000 wird durch den Eigentümer eines Objekts bestimmt. Für die verschiedenen Objekte des BS2000 stehen ihm je nach der Art des Objekts und der Art des Datenträgers unterschiedliche Zugriffsschutzmechanismen zur Verfügung. Die folgenden Ausführungen gelten uneingeschränkt für Dateien auf gemeinschaftlichen Plattenspeichern, jedoch zum Teil nur eingeschränkt für die weiteren Objekte des BS2000 (siehe Seite 130).

6.2.1 Grundlagen des Objektschutzes

Die wichtigste Grundlage des Objektschutzes bildet das Eigentümerrecht. Auf dem Eigentümerrecht setzen die Zugriffsschutzmechanismen und Schutzattribute des BS2000 auf.

Eigentümerrecht

Der Erzeuger eines Objekts ist auch ihr Eigentümer. Das Eigentümerrecht für ein Objekt ist immer an eine Benutzerkennung geknüpft. Es bezieht sich auf das Erzeugen, Ändern und Löschen eines Objekts sowie auf das Festlegen der Schutzattribute des Objekts.

In der Regel ist ein Objekt nur der Nutzung durch den Eigentümer vorbehalten. Für die Nutzung durch andere Benutzer müssen vom Eigentümer explizit Zugriffsrechte vergeben werden. Die Zugriffsschutzmechanismen des BS2000 gewährleisten, daß ein Benutzer nur auf die Objekte zugreifen kann, für die er eine Berechtigung besitzt.

Neben Objekten, für die der Zugriff durch den Eigentümer bestimmt wird, gibt es im BS2000 auch Objekte, für die kein Eigentümer existiert (z.B. MEMORY Pools). Für diese Objekte wird der Zugriffsschutz über spezifische Zugriffsrechte und Zugriffsschutzmechanismen geregelt (siehe Seite 130ff).

Ausnahmen des Zugriffsschutzes

Der Zugriffsschutz des BS2000 kann von der Systemverwaltung durchbrochen werden. Sie kann das Eigentümerrecht für alle Benutzerkennungen ersatzweise wahrnehmen. Überdies verfügt sie über spezielle Berechtigungen bei der Ausführung von Kommandos und Dienstprogrammen, z.B. kann die Systemverwaltung Kennwörter ignorieren.

Zugriff auf Dateien über den Dateikatalog

Nur katalogisierte Dateien sind dem BS2000 für eine Verarbeitung zugänglich. Für jede im Betriebssystem verfügbare Datei existiert deshalb ein Eintrag im Dateikatalog des entsprechenden Pubset. Eine Datei wird unter der Benutzerkennung des Auftrags katalogisiert, der sie erzeugt. Der Katalogeintrag enthält alle wesentlichen Informationen über die Datei: den Dateinamen, die vereinbarten Schutzattribute und weitere Dateiattribute bezüglich des Datenträgers und der Art der Speicherung.

Der Katalogeintrag kann nur vom Eigentümer der Datei (und von der Systemverwaltung) geändert werden. Beispielsweise kann der Eigentümer allen Benutzerkennungen, seine eigene eingeschlossen, Zugriffe auf eine Datei verbieten. Auch in diesem Fall ist er berechtigt den Katalogeintrag durch Setzen von Schutzattributen zu ändern und dadurch wieder Zugriffe auf die Datei zu erlauben.

Der Zugriff auf die Inhalte einer Datei erfolgt unter Berücksichtigung des zugehörigen Katalogeintrags. Dazu dient der Pfadname, der sich aus der Katalogkennung (CATID des Pubset), der Benutzerkennung und dem vollständigen Namen der Datei zusammensetzt. Für jeden Zugriff auf eine Datei wird überprüft, ob die gewünschte Datei existiert und die vereinbarten Schutzattribute den gewünschten Zugriff gestatten.

An der Benutzerschnittstelle wird der Pfadname aus Flexibilitäts- und Komfortgründen nicht in der vollständigen Form verlangt. Um sicherzustellen, daß keine Vertauschungen von Dateien auftreten, ergänzt das Betriebssystem fehlende Angaben und arbeitet intern immer mit dem vollständigen Pfadnamen. Zur Ergänzung des Pfadnamens wird die im Benutzerkennungskatalog des Home-Pubset angegebene Default-CATID verwendet, sowie beim Zugriff auf eine permanente Datei die im SET-LOGON-PARAMETERS-Kommando angegebene Benutzerkennung. Existiert eine im START-PROGRAM angegebene Datei unter der SET-LOGON-PARAMETERS-Benutzerkennung nicht, wird der Dateiname mit der Default-Userid ergänzt. Der Benutzer sollte sich allerdings bewußt sein, daß es sich um relative Namen handelt und im Zweifelsfall den Pfadnamen explizit angeben.

Einschränkung der Verfügbarkeit von Dateien

Die Verfügbarkeit kann dadurch eingeschränkt werden, daß

- die Datei in einem speziellen Betriebsmodus eröffnet wird oder
- die Datei durch das Kommando SECURE-RESOURCE-ALLOCATION (siehe Anhang A) exklusiv reserviert wird.

Bevor auf eine Datei durch den Programmlauf eines Benutzers zugegriffen werden kann, muß sie zuvor für die Verarbeitung eröffnet werden. Nachdem alle Lese- und Schreiboperationen durch den Programmlauf abgeschlossen sind, wird die Datei durch Schließen wieder für eine weitere Verarbeitung verfügbar.

Durch das Kommando SECURE-RESOURCE-ALLOCATION können Dateien und Datenträger, die eine Task für ihren Ablauf benötigt, exklusiv reserviert werden. Eine exklusive Reservierung ist nur möglich, wenn die Datei nicht eröffnet ist. Eine exklusiv reservierte Datei kann nur von der Task, die die Datei reserviert hat, eröffnet werden. Eine Reservierung wird aufgehoben durch:

- das Kommando REMOVE-FILE-LINK,
- das Kommando SECURE-RESOURCE-ALLOCATION ohne Operanden,
- das Kommando WAIT-EVENT und
- das Auftragsende.

Die Einschränkungen der Verfügbarkeit von Dateien gelten bis zur expliziten Freigabe und betreffen den Zugriff durch Programmläufe anderer Benutzer ebenso wie das Setzen oder Modifizieren von Schutzattributen durch den Eigentümer.

Gleichzeitige Bearbeitung von Dateien

Es kann erreicht werden, daß mehrere Aufträge gleichzeitig auf eine Datei zugreifen. Das BS2000 gewährleistet durch interne Schutzmechanismen, daß Aufträge, die gleichzeitig eine Datei bearbeiten wollen, sich nicht gegenseitig stören.

Die gleichzeitige Bearbeitung gibt es nur für die folgenden Fälle:

- Unter Berücksichtigung der Schutzattribute und in Abhängigkeit von der verwendeten Zugriffsmethode können mehrere Aufträge gleichzeitig lesend auf eine Datei zugreifen.
- Bei den Zugriffsmethoden ISAM und UPAM (siehe "BS2000 Technische Beschreibung- Dateiverwaltungssystem" [19]) können durch "Shared-Update-Verarbeitung" mehrere Aufträge gleichzeitig lesend und schreibend auf eine Datei zugreifen.

6.2.2 Prinzipien der Zugriffskontrolle

Dateien auf gemeinschaftlichen Plattenspeichern sind die wichtigsten Objekte des BS2000. Zum Schutz einer Datei bietet das BS2000 dem jeweiligen Eigentümer vier Schutzmechanismen an, die unterschiedlich die Mehrbenutzbarkeit und die Zugriffsrechte regeln und zueinander in der folgenden hierarchischen Beziehung stehen:

- der Zugriffsschutz über Zugriffsbedingungen, die unabhängig vom zu schützenden Objekt verwaltet werden (Generally Usable Access contRol aDminiStration: GUARDS). GUARDS erlaubt neben dem Schutz für Dateien auch den Schutz von FITC-Ports und Bibliothekselementen).
- die Zugriffskontrolliste für Dateien (Access Control List, ACL),
- die einfache Zugriffskontrolliste (Basic Access Control List, BASIC-ACL) und
- die Standard-Zugriffskontrolle (Schutzattribute ACCESS und USER-ACCESS).

Von den vier Schutzmechanismen wird genau ein Schutzmechanismus bei jeder Überprüfung einer Zugriffsberechtigung herangezogen, und zwar derjenige, der in der Hierarchie am höchsten steht und aktiviert ist. Die Schutzmechanismen Guard, ACL und BASIC-ACL sind standardmäßig deaktiviert und können explizit über Kommandos vom Eigentümer des Objekts aktiviert bzw. deaktiviert werden. Die Standard-Zugriffskontrolle für eine Datei ist genau dann aktiviert, wenn sowohl weder Guard-Schutz noch ACL oder BASIC-ACL aktiviert sind. Ein "Ausschalten" aller vier Schutzmechanismen ist nicht möglich.

Bei der Überprüfung der Zugriffsberechtigung wird folgendes Verfahren angewendet:

1) Ist als Schutzmechanismus GUARDS oder FACS für das Objekt eingetragen, wird der Schutzmechanismus zur Zugriffskontrolle herangezogen.
2) Ist weder ein Guard noch eine ACL als Schutzmechanismus eingetragen, jedoch die BASIC-ACL, wird die BASIC-ACL zur Zugriffskontrolle herangezogen.
3) Ist weder Guard, die ACL noch die BASIC-ACL aktiviert, werden die Schutzattribute ACCESS und USER-ACCESS zur Zugriffskontrolle herangezogen.

Zusätzlich zu allen Zugriffsschutzmechanismen gelten immer die Schutzmethoden mit Hilfe von Kennwörtern (Lese-, Schreib- und Ausführungskennwort) sowie der vom Systemverwalter TSOS einrichtbare begrenzte Pubsetzugriff.

Anmerkungen:

- Soll eine Datei durch die BASIC-ACL geschützt werden, ist der Eigentümer der Datei dafür verantwortlich, daß ACL und Guard deaktiviert ist.
- Soll eine Datei durch die Standard-Zugriffskontrolle geschützt werden, ist der Eigentümer der Datei dafür verantwortlich, daß Guard, ACL und BASIC-ACL deaktiviert sind.

Neben diesen drei Schutzmechanismen, die alternativ einsetzbar sind, gibt es noch Schutzattribute, die zusätzlich eingesetzt werden können:

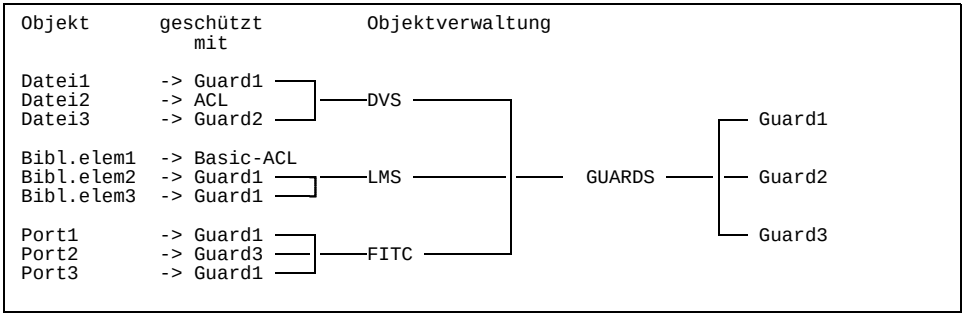
- die Schutzattribute für den Kennwortschutz:
  - WRITE-PASSWORD,
  - READ-PASSWORD,
  - EXEC-PASSWORD,
- das Schutzattribut DESTROY-BY-DELETE,
- das Schutzattribut AUDIT und
- das Schutzattribut RETENTION-PERIOD.

Weitere Schutzattribute, die allerdings objekt-spezifisch sind, werden im Zusammenhang mit der Steuerung des Zugriffsschutzes für die verschiedenen Objekte des BS2000 beschrieben (siehe Seite 130ff).

6.2.3 GUARDS - Zugriffsschutz für Objekte

Beim Zugriffsschutz mit Hilfe von GUARDS arbeiten Objektverwaltung und GUARDS zusammen. Die Objektverwaltungen stellen bei GUARDS die Anfrage, ob die Zugriffsbedingungen im Guard, dessen Name bei der Objektverwaltung als Referenz hinterlegt ist, für ein zugreifendes Subjekt zum Zeitpunkt des Zugriffs erfüllt sind. GUARDS wertet die Zugriffsbedingungen aus und gibt das Ergebnis "Bedingungen erfüllt" oder "Bedingungen nicht erfüllt" zurück. Dann entscheidet die Objektverwaltung, ob und wie ein Zugriff gestattet ist oder nicht.

Derselbe Guard-Name kann bei verschiedenen Objektverwaltungen hinterlegt sein. Es ist möglich, einen FITC-Port, ein Bibliothekselement und eine Datei mit einem einzigen Guard zu schützen. Auf diese Weise lassen sich leicht wartbare Sicherheitskonzepte mit einigen wenigen, zentralen Guards erstellen.



6.3 Arbeiten mit GUARDS

GUARDS ermöglicht den Schutz von Dateien, Bibliothekselementen und FITC-Ports gegen unberechtigte Zugriffe. Dateien, Bibliothekselemente und FITC-Ports sind Objekte von Objektverwaltungen. GUARDS stellt eine von den Objektverwaltungen unabhängige Bedingungsverwaltung und Bedingungsauswertung dar. Die Zugriffsbedingungen werden in den Objekten von GUARDS, den sogenannten Guards, hinterlegt, die über einen frei wählbaren Namen identifiziert werden. Die Verwendung von Zugriffsbedingungen ermöglicht einen differenzierteren Zugriffsschutz als die Vergabe von Zugriffsrechten z.B. über eine ACL.

Zum Arbeiten mit GUARDS gehören die folgenden Aspekte:

– Arbeiten mit Objekten, die mit Hilfe von GUARDS geschützt werden. Wird auf ein mit Hilfe von GUARDS geschütztes Objekt zugegriffen, ergibt die Auswertung der in Guards hinterlegten Zugriffsbedingungen, ob ein Zugriff gestattet wird oder nicht. Weitere Hinweise zu diesem Themenkreis finden Sie ab Seite 114.

– Einrichten und Verwalten des GUARDS-Schutzes.
  Dieser Abschnitt schildert den Ablauf einer Zugriffsbedingungsprüfung, beschreibt die logische Verknüpfung der Zugriffsbedingungen und erläutert die Schritte zum Erzeugen eines Guards, die Definition der von GUARDS auszuwertenden Bedingungen und die Zuweisung zum zu schützenden Objekt.

Jemand, der ein Guard einrichtet, ist dessen Eigentümer und hat alle Verwaltungsrechte. Die Kennung TSOS ist Miteigentümer aller Guards und darf sie deshalb ebenfalls verwalten.

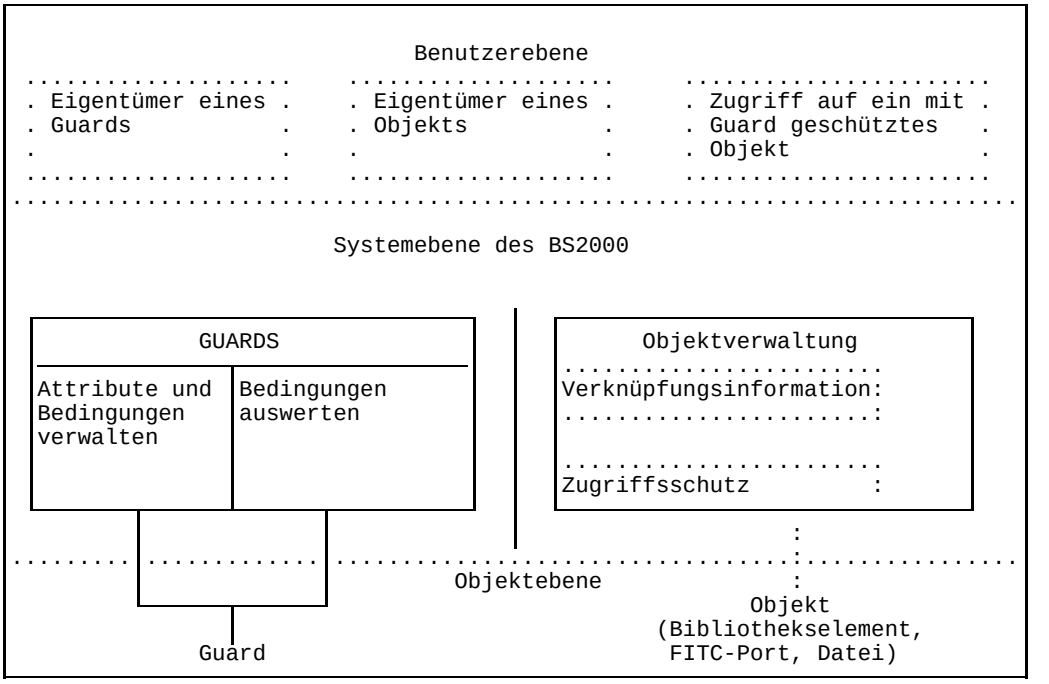


Bild 13: Bestandteile von GUARDS

Legende: ——— für den dargestellten Sachverhalt relevante Bestandteile
.... momentan nicht relevante Bestandteile oder Trennlinien

Das Bild zeigt die Beteiligten an der Verwirklichung eines Zugriffsschutzes für ein Objekt. GUARDS und die Objektverwaltungen der zu schützenden Objekte sind voneinander unabhängig. GUARDS gliedert sich in einen Teil zur Verwaltung der eigenen Objekte, den Guards, und einen anderen Teil zur Auswertung der in den Guards abgelegten Bedingungen.

Die Auswertung von Bedingungen wird auf Anfrage hin aufgerufen. Diese Anfragen können Objektverwaltungen stellen. Bei der jeweiligen Objektverwaltung ist hinterlegt, mit welchem Guard ein Objekt verknüpft ist. Die Verknüpfung veranlaßt der Eigentümer des Objekts über die betreffende Objektverwaltung. Objektverwaltungen, die ab BS2000 V11 GUARDS nutzen können, sind:

Objektverwaltung	**Objekt**
DVS (Dateiverwaltungssystem)	Dateien
LMS (Library Management System)	Bibliothekselemente
FITC (Fast Intertask Communication)	Ports

Die Zusammenarbeit zwischen GUARDS und einer dieser Objektverwaltungen läuft wie folgt ab (dieser Ablauf ist auch in Bild 30 festgehalten):

- Über eine Objektverwaltung soll auf ein von ihr verwaltetes Objekt zugegriffen werden (z.B. DVS: eine Datei).
- Bei der Objektverwaltung ist hinterlegt, welcher Zugriffsschutz verwendet werden soll. Wird GUARDS verwendet, ist für das Objekt vermerkt, in welchem Guard die Bedingungen enthalten sind.
- Die Objektverwaltung fragt bei GUARDS nach, wie die Antwort auf die Auswertung der bei GUARDS in dem mit dem Objekt verknüpften Guard gespeicherten Bedingungen lautet.
- GUARDS ermittelt, ob die Bedingungen erfüllt sind oder nicht, und gibt eine entsprechend lautende Antwort.
- Die Objektverwaltung entscheidet nun, ob ihre eigenen Regeln zusammen mit dem Ergebnis der GUARDS-Auswertung einen Zugriff gestatten (Bild 30) oder nicht (z.B. bei DVS wird als letztes das Ausführungs-, Lese- oder Schreibkennwort ausgewertet, sofern Kennwörter definiert sind).

Aufgrund der Unabhängigkeit von GUARDS zu anderen Objektverwaltungen ist es deshalb möglich, ein und dasselbe Guard von unterschiedlichen Objektverwaltungen aus zu verwenden, ohne das Guard zu ändern. Für eine Sicherheitskonzeption bedeutet dies, daß einige zentrale Guards eingerichtet werden können, um gut wart- und kontrollierbare Zugriffsbedingungen zu schaffen.

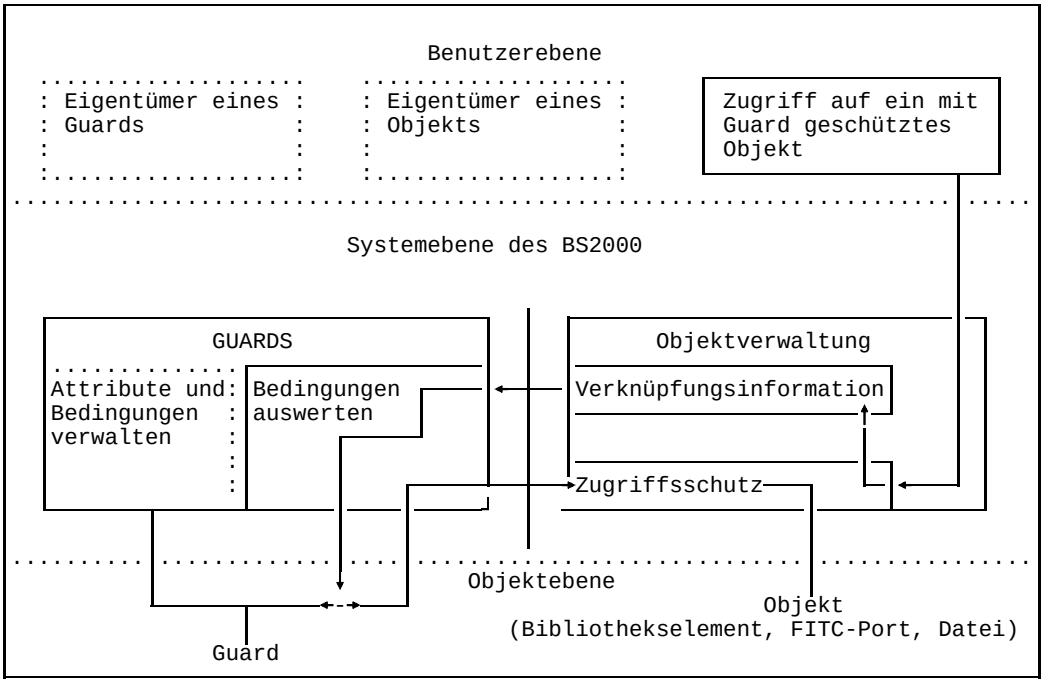


Bild 14: Ablauf bei Zugriff auf ein mit Hilfe von GUARDS geschütztes Objekt

Legende: ——— für den dargestellten Sachverhalt relevante Bestandteile
.... momentan nicht relevante Bestandteile oder Trennlinien

6.3.1 GUARDS-Schutz einrichten

Die Einrichtung des GUARDS-Schutzes umfaßt zwei Schritte:

– die Bereitstellung eines Guards, das die Bedingungsdefinitionen aufnehmen soll oder bereits enthält.

  Für die Verwaltung der Attribute der Guards stellt GUARDS Kommandos zur Verfügung, um Guards zu erstellen, die Attribute zu ändern, das Guard zu kopieren und anzuzeigen sowie das Guard zu löschen. In den betreffenden Kommandos wird ein Guard über seinen frei wählbaren Namen identifiziert.

  Für die Verwaltung der Bedingungen in den Guards stellt GUARDS die Kommandos zur Verfügung, um Bedingungen zu definieren, zu ändern oder zu löschen.

– Verknüpfung des Guards mit dem zu schützenden Objekt. Die Verknüpfungsinformation wird bei der Objektverwaltung des zu schützenden Objekts hinterlegt. Objektverwaltungen, die ihre Objekte mit Guards schützen können, erweitern ihre Schnittstellen der Attribut-Änderung ihrer Objekte, um die Verknüpfung herstellen zu können.

Guard einrichten und Zugriffsbedingungen definieren

Da zu schützendes Objekt und Guard voneinander unabhängig sind, werden sie in unabhängigen Arbeitsschritten bearbeitet. Bearbeitet werden Objekte und Guards von ihren Eigentümern. Objekt und Guard können verschiedene Eigentümer haben und so auch von verschiedenen Personen bearbeitet werden. Besondere Rechte sind an das Privileg TSOS gekoppelt. Die Kennung TSOS ist (Mit-) Eigentümer aller Guards und von GUARDS geschützten Objekten und darf deshalb auch alle Guards und Objekte bearbeiten.

Festlegen der Attribute eines Guard

Die Attribute des Guards legen fest, wer das Guard zum Schutz seiner Objekte verwenden darf (SCOPE-Attribut). Das Guard wird mit den Kommandos CREATE-GUARD oder COPY-GUARD eingerichtet, seine Attribute werden mit dem Kommando MODIFY-GUARD-ATTRIBUTES geändert. Das Guard wird mit DELETE-GUARD gelöscht. Der berechtigte Benutzer (festgelegt im SCOPE-Attribut des Guards) kann sich mit SHOW-GUARD-ATTRIBUTES die Attribute auch eines fremden Guards ansehen.

Festlegen von Zugriffsbedingungen

Zugriffsbedingungen werden mit dem Kommando ADD-ACCESS-CONDITIONS festgelegt und mit dem Kommando MODIFY-ACCESS-CONDITIONS geändert. REMOVE-ACCESS-CONDITIONS löscht Bedingungsdefinitionen in einem Guard.

Zur Anzeige der bestehenden Zugriffsbedingungen eines Guards stehen die Kommandos SHOW-ACCESS-CONDITIONS und SHOW-ACCESS-ADMISSION für den berechtigten Benutzer (festgelegt im SCOPE-Attribut des Guards) zur Verfügung.

Die Definition der Bedingungen kann die folgenden Aspekte enthalten:

– Zugriff generell gestattet oder nicht.
– Zugriff nur unter bestimmten Umständen gestattet:
  – Zeitraum (Uhrzeit, Datum, Wochentag) - es kann eine Liste von zulässigen Zeiträumen oder der Ausschluß bestimmter Zeiträume angegeben werden. Die Zeiträume sind untereinander mit dem logischen ODER verknüpft.

  – Privileg (nur für bestimmte Privilegien wird die Bedingung wahr) - es kann eine Liste von zulässigen Privilegien oder der Ausschluß bestimmter Privilegien angegeben werden. Die Privilegien in der Liste sind mit dem logischen ODER verknüpft.

– Programm (der Benutzer darf nur mit einem bestimmten Programm zugreifen, wobei GUARDS nicht nur überprüft, ob das Programm geladen ist, sondern ob es auch tatsächlich die Kontrolle hat). Die Programme in der Liste sind mit dem logischen ODER verknüpft.

Diese Aspekte können für verschiedene Subjekttypen (USER/GROUP/OTHERS/ ALL-USERS) in unterschiedlichen Ausprägungen optimal für den Schutzzweck festgelegt werden. Weitergehende Erläuterungen zur Auswertelogik für die Subjekttypen siehe Seite 110.

Verknüpfung Objekt - Guard

Erst wenn Guard und Objekt verknüpft sind, ist das Objekt mit Hilfe von GUARDS geschützt: es genügt nicht, ein Guard lediglich zu definieren. Nur der Eigentümer des zu schützenden Objekts kann diese Verknüpfung herstellen oder wieder lösen.

Mit Hilfe der jeweiligen Objektverwaltung (DVS, LMS, FITC) wird die Verknüpfung zwischen Objekt und Guard hergestellt. Diese Verknüpfung wird bei der jeweiligen Objektverwaltung, nicht aber bei GUARDS hinterlegt.

Ein Guard kann von mehreren Objektverwaltungen zum Schutz ihrer Objekte genutzt werden. Ebenfalls können mehrere Objekte durch ein Guard geschützt werden.

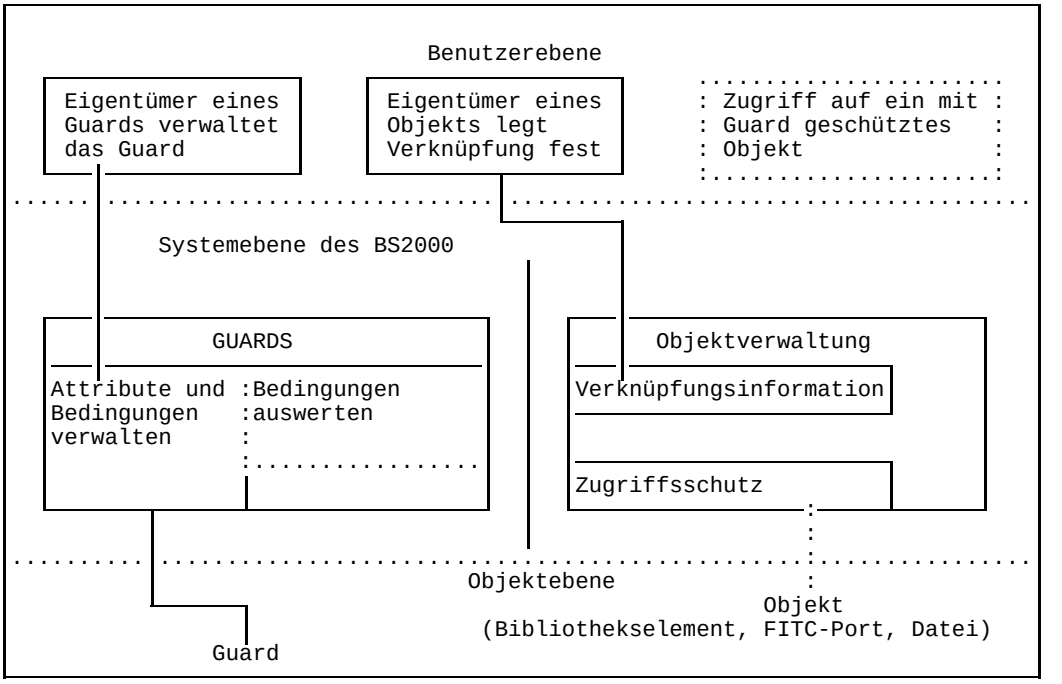


Bild 15: Verwaltungsaufgaben für Guard und Objekt

Legende: ——— für den dargestellten Sachverhalt relevante Bestandteile
.... momentan nicht relevante Bestandteile oder Trennlinien

Schutz der Objekte von DVS und LMS

Bei DVS wird der zum Schutz zu verwendende Guard-Name über den Operanden PROTECTION der Kommandos CREATE-FILE bzw. MODIFY-FILE-ATTRIBUTES mit der Datei verknüpft. Weitere Hinweise zur Einrichtung des Zugriffsschutzes für Dateien finden Sie im Handbuch zum DVS [9].

Beim LMS wird der zum Schutz zu verwendende Guard-Name mit den Anweisungen CREATE-ELEMENT bzw. MODIFY-ELEMENT-PROTECTION mit dem Bibliothekselement verknüpft. Weitere Hinweise zur Einrichtung des Zugriffsschutzes für Bibliothekselemente finden Sie im Handbuch zum LMS [24].

Bei DVS und LMS können Zugriffe auf ein Objekt je nach Zugriffsart (lesen, schreiben, ausführen) durch ein separates Guard geregelt werden. Die Objektverwaltung legt fest, ob es sich um einen Zugriff zum lesen, schreiben oder ausführen handelt. GUARDS hat keine Kenntnis vom Verwendungszweck.

Beim Einsatz von GUARDS werden von DVS und LMS nur Zugriffe gestattet, die explizit erlaubt sind. Im Gegensatz SHARE/ACCESS schließt bei GUARDS das Recht, schreibend zuzugreifen nicht auch das Recht, lesend zuzugreifen, ein.

Schutz des FITC-Ports

Bei FITC wird der zum Schutz zu verwendende Guard-Name über das Kommando PROTECT-FITC-APPLICATION mit dem Port verknüpft.

Hinweis

Bei der Definition von einzelnen Guards und der Verknüpfung der Objekte zu einem Guard muß genau überlegt werden, ob das Paar aus Zugriffsbedingung und Objekteigenschaften wirklich zusammenpaßt.

Beispiel:

Ein Benutzer hat eine Textdatei eingerichtet, in der der Quelltext für ein eigenes, kleines Programm enthalten ist. Dieser Quelltext soll nur einigen Benutzern zugänglich sein. Die Datei soll durch ein Guard geschützt werden.

Der Benutzer weiß, daß für seine Gruppe bereits ein Guard existiert, dessen Zugriffsdefinitionen genau den eigenen Vorstellungen entsprechen. Wenn er dieses (fremde) Guard verwendet, denkt sich der Benutzer, spart er sich die Definition eines eigenen Guards. Er weist der Datei das Guard GRPGUARD des Eigentümers XYZ zu mit dem Kommando MODIFY-FILE-ATTRIBUTES...,PROTECTION=PARAMETERS(READ=$XYZ.GRPGUARD,WRITE=$XYZ.GRPGUARD,EXEC=$XYZ.GRPGUARD).

Die Annahme, sich Arbeit gespart zu haben, ist nur so lange richtig, wie sich das Guard nicht ändert. Im Laufe der Zeit ergibt es sich, daß der Eigentümer des Guards die Definition so ändert, daß alle davon geschützten Dateien nur noch mit dem Privileg TAPE-ADMINISTRATION bearbeitet werden dürfen. Dies hat zur Folge, daß der Eigentümer der Programmdatei auf seine Datei nicht mehr zugreifen darf, da er nur das Privileg STD-PROCESSING besitzt. Um wieder zugreifen zu können, muß der Eigentümer die Zuweisung der Datei zu dem Guard lösen.

Dieses Beispiel soll verdeutlichen, welche Überlegungen vor Zuweisung eines Guards angestellt werden müssen, um eine Datei optimal zu schützen.

Rollen eines Benutzers

Das eben genannte Beispiel zeigt, daß der Eigentümer eines Objekts die Rolle wechselt.

Je nach dem, ob ein Objekt verwaltet oder auf ein Objekt zugegriffen werden soll, nimmt der Eigentümer eines Objekts unterschiedliche Rollen an:

Bei Objektverwaltungen:

Eigentümer verwaltet Objekt
Der Eigentümer verwaltet die Attribute des Objekts (Name, Schutzattribute etc.)

Eigentümer greift auf Objekt zu
Es gelten für ihn alle durch die Verwaltungsmaßnahmen festgelegten Zugriffsvorschriften.

Da GUARDS ebenfalls eine Objektverwaltung darstellt, verhalten sich die Objekte von GUARDS (die Guards) analog zu diesem Schema:

Bei GUARDS:

Eigentümer verwaltet Guard
Der Eigentümer des Guards verwaltet sein Guard. Er erzeugt, ändert, kopiert, löscht das Guard und legt Namen und Nutzungsberechtigung (SCOPE-Attribut) und Zugriffsbedingungen fest.

Eigentümer des Guard greift auf ein mit einem Guard geschütztes Objekt zu
Eigentümer spielt nun die Rolle eines "normalen" Benutzers. Somit gelten nun auch für ihn die im Guard abgelegten Zugriffsbedingungen.

Zugriff auf ein durch ein fremdes Guard geschütztes Objekt
Ein Benutzer darf den Schutz eines fremden Guards verwenden, wenn dies über das SCOPE-Attribut zugelassen ist. Da GUARDS erst im Augenblick der Auswertung etwas von der Verknüpfung bemerkt - die Verknüpfung ist bei der Objektverwaltung, nicht bei GUARDS hinterlegt - kann auch erst in diesem Augenblick von GUARDS geprüft werden, ob es sich um eine berechtigte Verknüpfung handelt. Das Ergebnis der Auswertung lautet "Bedingung nicht erfüllt" in folgenden Fällen:

- Das Guard existiert, aber das SCOPE-Attribut läßt eine Verwendung nicht zu.
- Das Guard existiert zum Zeitpunkt der Auswertung nicht (dies kann sein, weil es noch nicht definiert ist, die Verknüpfung erfolgte also vor der Erstellung des Guard oder es kann sein, weil ein zwar zum Zeitpunkt der Verknüpfung existierendes Guard in der Zwischenzeit gelöscht wurde).

6.3.2 Bedingungen für Subjekte definieren

Die Definition von Zugriffsbedingungen umfaßt zwei Schritte:

– festlegen, für welche Subjekttypen die Bedingungen gelten sollen. Subjekttypen sind USER, GROUP, OTHERS und das GUARDS-Pseudosubjekt ALL-USERS.

– Zugriffsbedingungen definieren.

Um Zugriffsbedingungen optimal formulieren zu können, ist die Kenntnis der Logik der Bedingungsauswertung unerläßlich. Für die Bedingungsauswertung ordnet GUARDS die Bedingungen und deren Auswertung nach Subjekttypen. Die Auswertung der Subjekttypen USER, GROUP und OTHERS wird abgebrochen, sobald der erste Treffer erzielt wurde. Die Auswertung kann immer nur eines von zwei Ergebnissen liefern: WAHR (Bedingungen sind erfüllt) oder FALSCH (Bedingungen sind nicht erfüllt).

Reihenfolge der Auswertung der Subjekttypen:

USER die Bedingungen von USER werden als erstes ausgewertet. Bei USER sind die Bedingungen hinterlegt, die explizit für eine Kennung (userid) gelten sollen. Als Parameter ist der Name einer Kennung, wie er mit ADD-USER festgelegt wurde, anzugeben. Bei der logischen Auswertung werden zuerst die Einträge für USER durchsucht, ob für die zur Prüfung anstehende Kennung ein Eintrag vorhanden ist. Wird eine Übereinstimmung gefunden, werden die für diese Kennung hinterlegten Bedingungen ausgewertet.

Lautet das Ergebnis der Auswertung WAHR, wird gleich mit der Auswertung der Bedingungen von ALL-USERS fortgefahren.

Lautet das Ergebnis der Auswertung der Bedingungen FALSCH, wird die Auswertung abgebrochen, und GUARDS übermittelt das Ergebnis FALSCH an die aufrufende Objektverwaltung.

GROUP spricht die Bedingungen an, die explizit für eine Benutzergruppe gelten sollen. Als Parameter ist der Name einer Benutzergruppe, wie er mit ADD-USER-GROUP festgelegt wurde, anzugeben. Bei der logischen Auswertung werden als zweites die Einträge für GROUP durchsucht, ob für die Gruppe, zu der die zur Prüfung anstehende Kennung gehört, ein Eintrag vorhanden ist. Wird eine Übereinstimmung gefunden, werden die für diese Gruppe hinterlegten Bedingungen ausgewertet.

Lautet das Ergebnis der Auswertung der Bedingungen WAHR, wird gleich mit der Auswertung der Bedingungen von ALL-USERS fortgefahren.

Lautet das Ergebnis der Auswertung der Bedingungen FALSCH, wird die Auswertung abgebrochen, und GUARDS übermittelt das Ergebnis FALSCH an die aufrufende Objektverwaltung.

OTHERS spricht die Bedingungen an, die für alle Subjekte gelten sollen, die nicht

durch Einträge für USER oder GROUP erfaßt worden sind.

Lautet das Ergebnis der Auswertung der Bedingungen WAHR, wird mit der Auswertung der Bedingungen von ALL-USERS fortgefahren.

Lautet das Ergebnis der Auswertung der Bedingungen FALSCH, wird die Auswertung abgebrochen und GUARDS übermittelt das Ergebnis FALSCH an die aufrufende Objektverwaltung.

Sind für eine zu prüfende Kennung weder Einträge bei USER noch bei GROUP vorhanden und sind in dem auszuwertenden Guard keine Einträge für OTHERS vorhanden, lautet das Ergebnis der Auswertung immer FALSCH.

ALL-USERS ist ein Pseudo-Subjekt, bei dem Bedingungen hinterlegt werden, die erst ausgewertet werden, wenn die vorher abgelaufene Prüfung für USER, GROUP oder OTHERS das Ergebnis WAHR geliefert hat. Wenn auch die für ALL-USERS hinterlegten Bedingungen zutreffen, lautet das Ergebnis der Auswertung WAHR. Wurden für ALL-USERS keine Bedingungen definiert, ist das Ergebnis der Auswertung der Bedingung für ALL-USERS immer WAHR.

Einträge für die Subjekttypen USER, GROUP, OTHERS und ALL-USERS sind optional. Wurden überhaupt keine Bedingungen definiert (das Guard ist also "leer"), lautet das Ergebnis der Auswertung immer, daß die Bedingungen nicht erfüllt sind. Ein leeres Guard existiert z.B. in der Zeit zwischen seiner Erzeugung mit dem Kommando CREATE-GUARD und der Definition der ersten Bedingung mit ADD-ACCESS-CONDITIONS oder nachdem alle Definitionen mit REMOVE-ACCESS-CONDITIONS gelöscht wurden.

Da die Bedingungen für ALL-USERS als letzte ausgewertet werden, geben die Definitionen bei ALL-USERS letztendlich den Ausschlag, ob die gesamte Auswertung das Ergebnis WAHR oder FALSCH bekommt.

Einträge bei ALL-USERS können dazu genutzt werden, Bedingungen in einem Zug für alle Subjekte im Guard festzulegen. So ist es möglich, durch einen Eintrag bei ALL-USERS den Zugriff auf ein Objekt generell zu sperren (MODIFY-ACCESS-CONDITIONS SUBJECT=ALL-USERS, ADMISSION=NO) oder gegebenenfalls wieder freizugeben (ADMISSION= YES oder ADMISSION=PARAMETERS(...)).

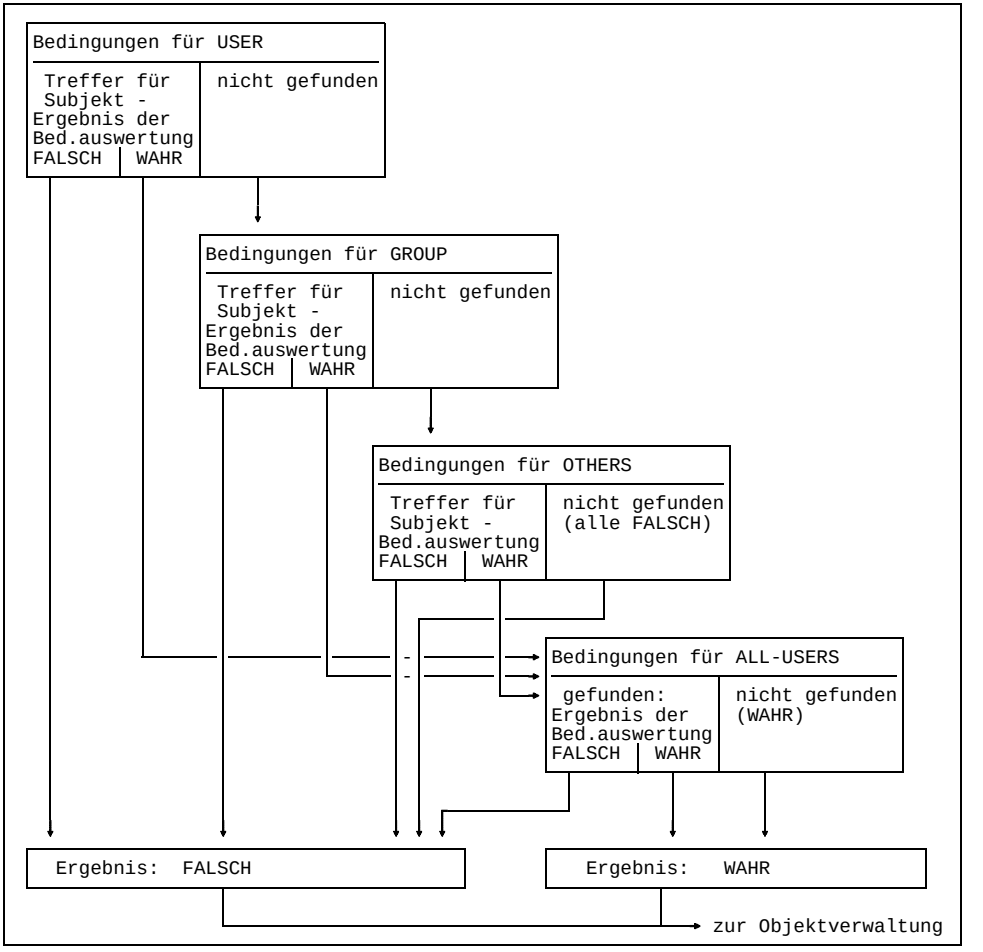


Bild 16: Logische Auswertung der Zugriffsbedingungen nach Subjekttyp

i Geben Sie acht, wenn Zugriffsbedingungen Entsprechungen sowohl bei ALL-USERS als auch bei USER, GROUP oder OTHERS finden, ob die Verknüpfung mit dem logischen UND zwischen ALL-USERS und den anderen Subjekten zum gewünschten Ergebnis führt.

Beispiel
Stecken Zugriffsbedingungen für eine einzelne Kennung (Subjekttyp USER) einen bestimmten Zeitrahmen ab, der nicht innerhalb des Zeitrahmens der Definition bei ALL-USERS liegt, wurden widersprüchliche Angaben gemacht, die dazu führen können, daß die Antwort von GUARDS negativ ausfällt, obwohl die Zugriffsbedingungen für das USER-, GROUP- oder OTHERS-Subjekt alle erfüllt sind, der Zeitpunkt des Zugriffs aber nicht im Zeitrahmen der ALL-USERS-Bedingung liegt. Die Verknüpfung mit den Bedingungen bei ALL-USERS über das logische UND führt zu dieser Reaktion (z.B. Zugriffsbedingung wird WAHR, wenn gilt: USER-Bedingung=WAHR UND ALL-USER-Bedingung=WAHR; Das Ergebnis der Auswertung lautet FALSCH, wenn gilt ALL-USER-Bedingung=FALSCH, weil mit ihr z.B. ein anderer Zeitrahmen abgesteckt wird).

Diese Reaktion kann gewünscht sein, um ein Objekt zu sperren. Sollte ein mit Hilfe von GUARDS geschütztes Objekt trotz korrekter Definition der Bedingungen für einen USER nicht zugreifbar sein, müssen auch die Definitionen für ALL-USERS überprüft werden.

GUARDS überprüft bei der Definition nicht, ob widersprüchliche Angaben in einem Guard hinterlegt sind.

Beispiel für die Verwendung von ALL-USERS

Auf eine Datei soll nur mit Hilfe des Editors EDT zugegriffen werden können. Obwohl weder für USER noch für GROUP noch für OTHERS ein Programm vorgesehen ist, wird der Zugriff dann aber über die Bedingungen von ALL-USERS geregelt.

Definition für USER:

```
add-access-conditions guard-name=guardexa,
                      subjects=user(user-identification=edtuser),
                      admission=yes
```

Definition für GROUP:

```
add-access-conditions guard-name=guardexa,
                      subjects=group(group-identification=edtgroup),
                      admission=parameters(privilege=std-processing)
```

Definition für OTHERS:

```
add-access-conditions guard-name=guardexa,
                      subjects=others,admission=yes
```

Definition für ALL-USERS:

```
add-access-conditions subjects=all-users,admission=parameters(program=$edt)
```

Ausgehend von der obigen Beispielsdefinition wird für die Kennung EDTUSER die Liste der möglichen Programme geändert:

```
modify-access-conditions subjects=user(user-identification=edtuser),
                         admission=parameters(program=($edt,$sort))
```

Die Definitionen für ALL-USERS gelten weiterhin. Für den Benutzer unter der Kennung EDTUSER sind die Bedingungen weiterhin WAHR, wenn er mit dem Programm EDT auf die mit Hilfe von GUARDS geschützte Datei zugreift. Wenn er versucht, auf die Datei mit dem Programm SORT zuzugreifen, wird die Auswertung der Bedingungen durch GUARDS dennoch das Ergebnis FALSCH liefern, da die Bedingungen für ALL-USERS nur den Zugriff mit EDT zulassen. GUARDS überprüft die Bedingungen in einem Guard nicht auf Folgerichtigkeit. Der Eigentümer des Guards muß selbst beurteilen, ob Unstimmigkeiten dieser Art gewollt sind oder nicht.

6.3.3 Arbeiten mit Objekten, die mit Hilfe von GUARDS geschützt werden

Ein Benutzer kann mit Dateien, Bibliotheken, Bibliohekselemente und FITC-Ports arbeiten, die mit Hilfe von GUARDS geschützt werden.

Dateien, die mit GUARDS geschützt werden, können nicht gleichzeitig durch ACCESS/USER-ACCESS, eine Basic-ACL oder ACL geschützt werden.

Zusätzlich zum GUARDS-Schutz können z.B. Kennwörter oder administrative Maßnahmen wie z.B. begrenzter Pubset-Zugang den Zugriff auf ein Objekt verhindern.

Für den Benutzer verändert sich das Verhalten seiner gewohnten Systemumgebung insoweit, daß jetzt unterschiedliche Objekte gegen unberechtigte Zugriffe geschützt sein können. Dies kann bedeuten, daß er durch den Einsatz von GUARDS nur noch unter bestimmten Bedingungen auf ein Objekt zugreifen darf. Sind zum Zeitpunkt des Zugriffs die bei GUARDS hinterlegten Bedingungen erfüllt und verweigern nicht andere Schutzmöglichkeiten (z.B. Kennwörter, beschränkter Pubset-Zugang etc.) den Zugriff, wird der Zugriff gestattet.

6.4 Zugriffskontrolliste (ACL)

Analog zum Benutzer- und zum Dateikatalog existiert auf jedem Pubset eine ACL-Datei, in der die Zugriffsrechte auf Dateien des gleichen Pubset in Form von Zugriffskontrollisten gespeichert sind. Für eine Datei kann höchstens eine ACL erzeugt und in die ACL-Datei eingetragen werden. Das Erzeugen einer ACL erfolgt nicht automatisch, sondern der Eigentümer einer Datei kann bestimmen, ob für die Datei eine ACL erzeugt wird oder nicht. Eine ACL kann - ebenfalls vom Eigentümer der Dateijederzeit gelöscht werden. Die Benutzerkennung TSOS kann für alle Dateien Zugriffskontrollisten erzeugen, ändern und löschen.

Durch Zugriffskontrollisten kann der Zugriffsschutz für Dateien bis auf die Ebene eines Benutzers verfeinert werden. Zugriffskontrollisten basieren auf dem Erlaubnisprinzip, d.h. die Zugriffe auf ein Objekt müssen explizit erlaubt werden, andernfalls sind sie grundsätzlich verboten.

Es bedeutet:

- "Die ACL für die Datei ’ABC’ ist aktiviert", daß über die Kommando- bzw. die Programmieroberfläche eine ACL für die Datei mit dem Dateinamen ’ABC’ erzeugt wurde und diese ACL nach wie vor vorhanden ist.
- "Die ACL für die Datei ’ABC’ ist deaktiviert", daß keine ACL für die Datei mit dem Dateinamen ’ABC’ vorhanden ist, entweder weil keine ACL erzeugt wurde oder weil eine vorhandene ACL über die Kommando- bzw. die Programmieroberfläche gelöscht wurde.

Für Dateien können folgende drei Zugriffsrechte vereinbart werden:

- Lesen,
- Schreiben und
- Ausführen.

Eine ACL für eine Datei besteht aus den folgenden vier Hauptteilen:

- dem Dateinamen,
- einer Liste von Benutzerkennungen und die ihnen zugeordneten Zugriffsrechte,
- einer Liste von Gruppenkennungen und die ihnen zugeordneten Zugriffsrechte, wobei die Gruppenzugehörigkeit aus der Benutzergruppenstruktur des Home-Pubset ermittelt wird,
- den standardmäßig gültigen Zugriffsrechten (Default Access Rights, Other).

Beispiel einer ACL:

Bild 13 zeigt eine ACL für eine Datei file1, wobei die Liste der Benutzerkennungen aus den Benutzerkennungen user5 und user6, die Liste der Gruppenkennungen aus den Gruppenkennungen group1 und der Universalgruppe besteht.

Die einzelnen Zeichen eines Zugriffsrechtetripels haben folgende Bedeutung:

R Zugriffsrecht 'Lesen' vereinbart,
W Zugriffsrecht 'Schreiben' vereinbart,
X Zugriffsrecht 'Ausführen' vereinbart,
– kein Zugriffsrecht für Lesen, Schreiben oder Ausführen vereinbart.

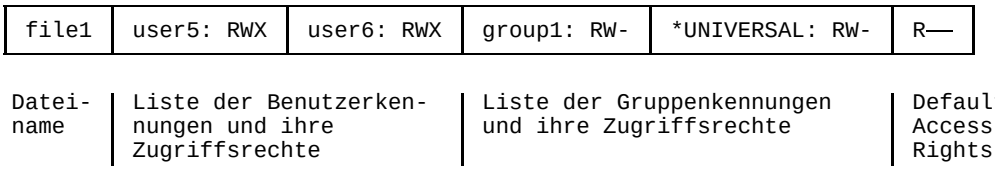


Bild 17: Beispiel einer ACL für eine Datei file1

Dateiname: file1

Liste der Benutzerkennungen und ihre Zugriffsrechte:

user5 : RWX berechtigt die Benutzerkennung user5 zum Lesen, Schreiben und Ausführen der Datei file1.

user6 : RWX berechtigt die Benutzerkennung user6 zum Lesen, Schreiben und Ausführen der Datei file1.

Liste der Gruppenkennungen und ihre Zugriffsrechte:

group1: RW- berechtigt alle Benutzerkennungen, die der Benutzergruppe group1 des Home-Pubset der laufenden BS2000-Sitzung angehören, zum Lesen und Schreiben, jedoch nicht zum Ausführen der Datei file1.

*UNIVERSAL:
RW- berechtigt alle Benutzerkennungen, die der Universalgruppe des Home-Pubset der laufenden BS2000-Sitzung angehören, zum Lesen und Schreiben, jedoch nicht zum Ausführen der Datei file1.

Default Access Rights:
R-- berechtigt alle Benutzerkennungen zum Lesen, jedoch nicht zum Schreiben und Ausführen der Datei file1.

Auswertung einer ACL

Die tatsächliche Zugriffsberechtigung einer Benutzerkennung für eine Datei wird folgendermaßen festgestellt, wobei grundsätzlich die Benutzergruppenstruktur des Home-Pubset der laufenden BS2000-Sitzung für die Überprüfung herangezogen wird:

1) Ist die Benutzerkennung, die den Zugriff wünscht, in der Liste der Benutzerkennungen enthalten, gelten die mit der Benutzerkennung abgespeicherten Zugriffsrechte.
2) Ist die Benutzerkennung nicht in der Liste der Benutzerkennungen enthalten, jedoch ihre Gruppenkennung in der Liste der Gruppenkennungen, gelten die mit der Gruppenkennung abgespeicherten Zugriffsrechte.
3) Ist die Benutzerkennung weder in der Liste der Benutzerkennungen noch ihre Gruppenkennung in der Liste der Gruppenkennungen enthalten, wird der Other-Eintrag ausgewertet.

Anmerkungen:

- Jede Benutzerkennung hat in einer ACL genau einen "Treffer": entweder in der Liste der Benutzerkennungen oder in der Liste der Gruppenkennungen, oder es gilt der Other-Eintrag.
- Es ist nicht erforderlich, daß der Eigentümer der Datei in der Liste der Benutzerkennungen enthalten ist. Es ist auch möglich, daß der Eigentümer der Datei keine Zugriffsrechte auf seine eigene Datei besitzt. Er hat jedoch auch dann die Berechtigung, sich die gewünschten Zugriffsrechte zuzuteilen.
- Für die Benutzerkennung TSOS gelten beim Zugriff auf fremde Dateien genauso wie für andere Benutzerkennungen die Rechte, die für TSOS, seine Gruppe oder für OTHERS vergeben sind. Für TSOS gelten also nicht die Zugriffsrechte des Eigentümers einer Datei. Allerdings kann TSOS als Miteigentümer die gewünschten Rechte setzen, ändern oder löschen.
- Die Liste der Benutzerkennungen und die Liste der Gruppenkennungen können auch leer sein.
- Der Other-Eintrag ist immer vorhanden.
- Das Zugriffsrecht ’Schreiben’ berechtigt nur zum Schreiben einer Datei, nicht aber zum Lesen (im Gegensatz zum Schutzattribut ACCESS, siehe Seite 124). Soll eine Datei zum Lesen und Schreiben eröffnet werden, müssen in der ACL die Zugriffsberechtigungen für Lesen und Schreiben gesetzt werden.

Beispiel einer ACL:

Gegeben sei die folgende Benutzergruppenstruktur (siehe Seite 51), festgelegt auf dem Home-Pubset der laufenden BS2000-Sitzung:

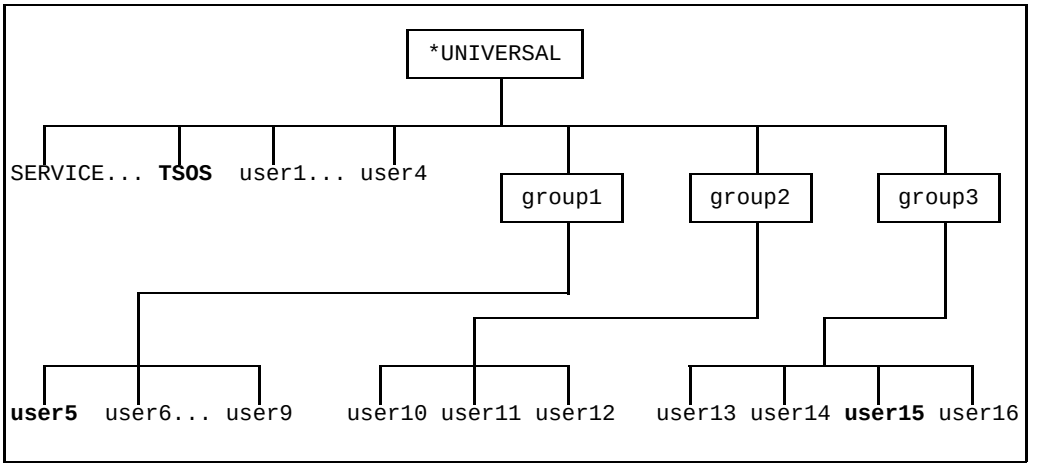


Bild 18: Benutzergruppenstruktur

Es sei folgende ACL-Datei mit den Zugriffskontrollisten von fünf Dateien auf einem Daten-Pubset vorhanden:

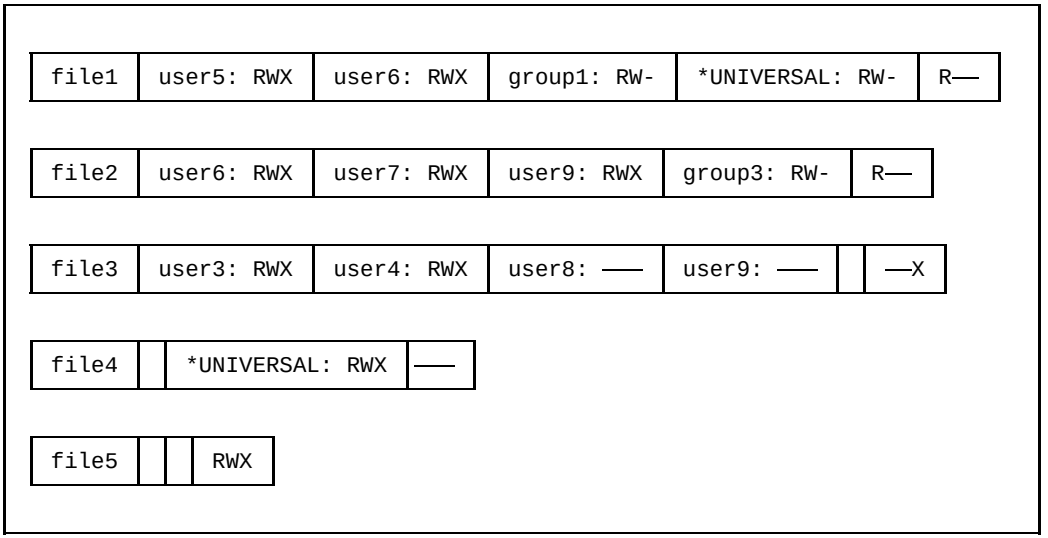


Bild 19: Beispiel einer ACL-Datei mit den Zugriffskontrollisten für fünf Dateien

Bild 16 zeigt welche Zugriffsrechte die Benutzerkennungen user5, user9, user10 und user15 auf die Dateien, die durch die Zugriffskontrollisten von Bild 15 geschützt sind, besitzen und welcher Eintrag in einer ACL (= ACL-Eintrag) die jeweiligen Zugriffsrechte bestimmt.

Benutzer-kennung	Datei-name	Zugriffsrechte	zutreffender Eintrag
user3	file1	Lesen, Schreiben	*UNIVERSAL in Liste der Gruppenkennungen
	file2	Lesen	Other
	file3	Lesen, Schreiben, Ausführen	user3 in Liste der Benutzerkennungen
	file4	Lesen, Schreiben, Ausführen	*UNIVERSAL in Liste der Gruppenkennungen
	file5	Lesen, Schreiben, Ausführen	Other
user9	file1	Lesen, Schreiben	group1 in Liste der Gruppenkennungen
	file2	Lesen, Schreiben, Ausführen	user9 in Liste der Benutzerkennungen
	file3	keine	user9 in Liste der Benutzerkennungen
	file4	keine	Other
	file5	Lesen, Schreiben, Ausführen	Other
user10	file1	Lesen	Other
	file2	Lesen	Other
	file3	Ausführen	Other
	file4	keine	Other
	file5	Lesen, Schreiben, Ausführen	Other
user15	file1	Lesen	Other
	file2	Lesen, Schreiben	group3 in Liste der Gruppenkennungen
	file3	Ausführen	Other
	file4	keine	Other
	file5	Lesen, Schreiben, Ausführen	Other

Bild 20: Zugriffsrechte der Benutzerkennungen user5, user9, user10 und user15

Auswirkungen des Löschens von Subjekten auf eine ACL

Beim Löschen von Benutzerkennungen bzw. von Benutzergruppen auf dem Home-Pubset der laufenden BS2000-Sitzung durch die Benutzerverwaltung werden die ACL-Einträge auf Daten-Pubsets nicht automatisch aktualisiert. Das bedeutet, daß ACL-Einträge auch Namen von Benutzerkennungen und Benutzergruppen enthalten können, die im Betriebssystem nicht mehr existieren. Das BS2000 verhindert nicht, daß Benutzerkennungen und Benutzergruppen unter früheren Namen neu eingerichtet werden können, wenn der vorgesehene Name noch in einer ACL enthalten ist.

Empfehlung:

Wird eine Benutzerkennung nicht mehr benötigt und ist auszuschließen, daß zu einem späteren Zeitpunkt unter dem gleichen Namen eine neue Benutzerkennung eingerichtet werden kann, die evtl. noch vorhandene Zugriffsrechte ihres "Vorgängers" übernimmt, so sollte die Benutzerkennung nicht gelöscht, sondern gesperrt werden.

6.5 Einfache Zugriffskontrolliste (BASIC-ACL)

Aufbauend auf dem Konzept der Benutzergruppen werden Zugriffsklassen für den Zugriff auf Objekte festgelegt. Die Zugriffsklassen unterteilen die Menge aller Benutzer jeweils in die Teilmengen OWNER, GROUP und OTHERS. Dabei bezeichnet:

- OWNER den Eigentümer eines Objekts,
- GROUP die Benutzergruppe des Home-Pubset der laufenden BS2000-Sitzung, der der Eigentümer angehört,
- OTHERS alle übrigen Benutzer.

Die Klassifizierung der Benutzer erfolgt stets individuell aus der Sicht des Eigentümers eines Objekts. Bezüglich eines Objekts sind die Zugriffsklassen OWNER, GROUP und OTHERS immer disjunkte Mengen von Benutzern.

Eine BASIC-ACL legt neun Zugriffsberechtigungen für eine Datei fest, indem sie der Datei drei Zugriffsrechte

- Lesen,
- Schreiben und
- Ausführen

für jede der drei Zugriffsklassen

- OWNER,
- GROUP und
- OTHERS

separat zuordnet.

Auswertung der BASIC-ACL

Es wird folgendes Verfahren angewendet, wobei grundsätzlich die Benutzergruppenstruktur des Home-Pubset der laufenden BS2000-Sitzung für die Zugriffsüberprüfung herangezogen wird:

1) Ist die Benutzerkennung, die den Zugriff wünscht, der Eigentümer des Objekts, gelten die unter OWNER abgespeicherten Zugriffsrechte.
2) Gehört die Benutzerkennung der Benutzergruppe des Eigentümers an, gelten die unter GROUP abgespeicherten Zugriffsrechte.
3) Für alle anderen Benutzerkennungen gelten die unter OTHERS abgespeicherten Zugriffsrechte.

Beispiele

Die Angabe der Zugriffsrechte erfolgt analog zur ACL. Für eine Datei können z.B. die folgenden Zugriffsberechtigungen vereinbart werden:

```
OWNER   GROUP   OTHERS

RWX     RWX     RWX       berechtigt den Eigentümer der Datei, die
                          Benutzergruppe auf dem Home-Pubset der
                          laufenden BS2000-Sitzung, zu der der
                          Eigentümer gehört, und alle übrigen Benutzer
                          zum Lesen, Schreiben und Ausführen der Datei.
RWX     R-X     R - -     berechtigt den Eigentümer der Datei zum
                          Lesen, Schreiben und Ausführen, die
                          Benutzergruppe, zu der der Eigentümer gehört,
                          zum Lesen und Ausführen
                          und alle übrigen Benutzer nur zum Lesen.
```

6.6 Standard-Zugriffskontrolle

Standard-Zugriffskontrolle durch den Einsatz der Schutzattribute ACCESS und USER-ACCESS bietet sich in den Fällen an, wo ein dedizierter Zugriffsschutz durch die ACL bzw. die BASIC-ACL nicht gewünscht wird.

Schutzattribut ACCESS

Durch Setzen des Schutzattributs ACCESS kann Schreibzugriff oder nur Lesezugriff für eine Datei erlaubt werden. Der Schreibzugriff impliziert dabei den Lesezugriff (im Unterschied zum Zugriffsrecht 'Schreiben' bei der ACL und der BASIC-ACL).

Schutzattribut USER-ACCESS

Mit dem Schutzattribut USER-ACCESS kann festgelegt werden, ob auf eine Datei nur der Eigentümer oder auch alle übrigen Benutzer (ausschließlich oder einschließlich der Benutzerkennung SERVICE für die Online-Wartung) zugreifen dürfen.

Anmerkung:

Ein Dateizugriff wird einer Kennung mit dem Privileg HARDWARE-MAINTAINANCE (bei Auslieferung hat dies die Kennung SERVICE) nur dann erlaubt, wenn

- die ACL oder ein Guard den Zugriff nicht verbietet,
- die BASIC-ACL den Zugriff nicht verbietet und
- USER-ACCESS=SPECIAL gesetzt ist.

6.7 Schutzattribute für den Kennwortschutz

Schutzattribute für den Kennwortschutz können zusätzlich zu den oben erwähnten Schutzmechanismen für verschiedene Objekte des BS2000 eingesetzt werden. Der Kennwortschutz basiert im Gegensatz zum Guard, zur ACL und zur BASIC-ACL auf dem Verbotsprinzip. Der Zugriff auf ein Objekt ist grundsätzlich erlaubt, wenn er nicht explizit verboten wurde. Eine Zugriffserlaubnis wird nur dann erteilt, wenn das vom Eigentümer des Objekts festgelegte Kennwort vor dem Zugriff korrekt angegeben wurde. Durch Kennwörter kann der Eigentümer gezielt Zugriffsrechte für Objekte einschränken.

Jeder Task wird eine interne Kennworttabelle zugeordnet, in die der Benutzer über die Kommandoschnittstelle Kennwörter eintragen kann. Zusätzlich gibt es die Möglichkeit, benötigte Kennwörter direkt über die Kommandoschnittstelle (z.B. beim Kommando DELETE-FILE) bzw. die Programmschnittstelle (z.B. beim Makro FCB) anzugeben. Bei einem Zugriff auf ein durch ein Kennwort geschütztes Objekt sucht das BS2000 das benötigte Kennwort in der Kennworttabelle, im Kommando bzw. im Makro. Wird das korrekte Kennwort gefunden, wird der Zugriff auf das Objekt freigegeben, sofern nicht andere Schutzattribute bzw. -mechanismen den Zugriff verhindern.

Kennwörter werden derzeit aus maximal vier alphanumerischen, maximal acht dezimalen oder maximal acht hexadezimalen Zeichen gebildet. Um trotz der großen Variationsbreite ein rechnerunterstütztes Ausprobieren von Kennwörtern zu verhindern, existieren Schutzschranken für Kennwörter:

- die Größe der internen Kennworttabelle,
- die Anzahl der erlaubten Kennwörter je Prozeß und
- die Anzahl der erlaubten Fehlversuche bei der Kennworteingabe.

Alle von einem Prozeß benötigten Kennwörter können in der internen Kennworttabelle des Auftrags bereitgestellt werden. Die Einschränkung der Größe der Kennworttabelle bewirkt, daß nicht beliebig viele Kennwörter abgespeichert und für einen Vergleich herangezogen werden können.

Die Anzahl der von einem Prozeß in die Kennworttabelle eintragbaren Kennwörter kann auf einen frei wählbaren Wert beschränkt werden, der z.B. der Anzahl der insgesamt in dem Prozeß verwendeten Kennwörter entspricht.

Das BS2000 zählt bei jeder Überprüfung der Übereinstimmung von Kennwörtern die festgestellten Fehlversuche mit. Beim Überschreiten eines vorgegebenen Grenzwertes wird der verursachende Prozeß zwangsweise mit einer Meldung an den Benutzer und die Systemverwaltung abgebrochen. Um das Ausprobieren von Kennwörtern zu erschweren, kann von der Systemverwaltung eine Verzögerungszeit von bis zu 60 Sekunden vorgegeben werden. Die Verzögerungszeit wird zusammen mit der Anzahl der bereits erfolgten Fehlversuche zur Berechnung einer task-spezifischen Zeitstrafe verwendet. Bei einem Fehlversuch wird die Zeitstrafe verhängt. Der Auftrag wird bis zum Ablauf der Zeitstrafe unterbrochen; erst dann ist die Wiederholung des Versuchs möglich.

Kennwort-Verschlüsselung

Um das Lesen von gespeicherten Kennwörtern zu verhindern, bietet das BS2000 die Möglichkeit der Kennwort-Verschlüsselung an. Bei der Systemgenerierung wird festgelegt, ob Kennwörter verschlüsselt werden. Das angewendete Verschlüsselungsverfahren ist eine Einwegverschlüsselung.

Jedes Kennwort, das ein Benutzer für eine Datei vereinbart, wird in verschlüsselter Form gespeichert. Eine Entschlüsselung des vereinbarten Kennworts ist nicht möglich. Vor einem Zugriff auf die Datei muß der Benutzer ein vereinbartes Kennwort in die Kennworttabelle des Auftrags eintragen. Das eingetragene Kennwort wird ebenfalls verschlüsselt und liefert ein Vergleichskennwort. Das so gewonnene Vergleichskennwort wird mit dem gespeicherten Kennwort verglichen. Bei Übereinstimmung der beiden verschlüsselten Kennwörter wird der Zugriff auf die Datei freigegeben, wenn der Auftrag alle weiteren Zugriffsrechte bereits besitzt.

Durch die Einwegverschlüsselung ist auch bei Kenntnis eines abgespeicherten (verschlüsselten) Kennworts ein Überwinden des Kennwortschutzes nur mit sehr hohem Rechenaufwand möglich.

Kennworthierarchie

Kennwörter unterliegen der folgenden hierarchischen Rangfolge:
Schreibkennwort → Lesekennwort → Ausführungskennwort. Die sich aus dieser Rangfolge ergebenden Möglichkeiten der Kennwortvereinbarung und die jeweils geltenden Zugriffsrechte sind in Bild 17 dargestellt. Um vereinbarte Kennwörter ändern zu können, muß der Benutzer das jeweilige Zugriffsrecht entsprechend der Rangfolge der Kennwörter besitzen. Sind mehrere Kennwörter für ein Objekt vereinbart, ist bei der Änderung eines Kennworts die Angabe der in der Rangfolge untergeordneten Kennwörter nicht erforderlich (z.B. ist die Angabe des Lesekennworts nicht erforderlich bei der Änderung des Schreibkennworts).

Kennwortschutz	Kennwortangabe	Zugriffsmöglichkeit
EXEC-PASSWORD	keine Angabe	kein Zugriff
	Ausführungskennwort	Ausführen Lesen Schreiben
READ-PASSWORD	keine Angabe	Ausführen
	Lesekennwort	Ausführen Lesen Schreiben
WRITE-PASSWORD	keine Angabe	Ausführen Lesen
	Schreibkennwort	Ausführen Lesen Schreiben
EXEC-PASSWORD READ-PASSWORD	keine Angabe	kein Zugriff
	Ausführungskennwort	Ausführen
	Lesekennwort	Ausführen Lesen Schreiben
EXEC-PASSWORD WRITE-PASSWORD	keine Angabe	kein Zugriff
	Ausführungskennwort	Ausführen Lesen
	Schreibkennwort	Ausführen Lesen Schreiben

Kennwortschutz	Kennwortangabe	Zugriffsmöglichkeit
READ-PASSWORD WRITE-PASSWORD	keine Angabe	kein Zugriff
	Lesekennwort	Ausführen Lesen
	Schreibkennwort	Ausführen Lesen Schreiben
EXEC-PASSWORD READ-PASSWORD WRITE-PASSWORD	keine Angabe	kein Zugriff
	Ausführungskennwort	Ausführen
	Lesekennwort	Ausführen Lesen
	Schreibkennwort	Ausführen Lesen Schreiben

Bild 21: Zugriffsrechte beim Kennwortschutz

Schutzattribut WRITE-PASSWORD

Durch Setzen des Schutzattributs WRITE-PASSWORD kann der Eigentümer ein Kennwort zum Schutz vor unberechtigtem Schreiben für eine Datei festlegen.

Ein Schreibkennwort für eine Datei muß explizit durch den Eigentümer vereinbart werden. Das vereinbarte Kennwort muß in die interne Kennworttabelle des Auftrags eingetragen werden, damit ein Schreibzugriff auf die Datei möglich ist. Ein in die Kennworttabelle eingetragenes Kennwort berechtigt auch zum Zugriff auf andere Dateien, für die dieses Kennwort vereinbart wurde, und zwar solange, bis es explizit aus der Kennworttabelle des Auftrags gelöscht wird oder bei Auftragsende, wenn die Kennworttabelle implizit gelöscht wird.

Schutzattribut READ-PASSWORD

Durch Setzen des Schutzattributs READ-PASSWORD kann der Eigentümer ein Kennwort zum Schutz vor unberechtigtem Lesen für eine Datei festlegen.

Ist ein Programm durch ein Lesekennwort geschützt, so kann auf den Programmcode nicht zugegriffen werden.

Der Zugriff auf eine Datei, die vor unberechtigtem Lesen geschützt ist, erfolgt analog zum Schutzattribut WRITE-PASSWORD.

Schutzattribut EXEC-PASSWORD

Durch Setzen des Schutzattributs EXEC-PASSWORD kann der Eigentümer ein Kennwort zum Schutz vor unberechtigtem Ausführen für eine Datei (die z.B. eine Prozedur oder ein Lademodul enthält) festlegen.

Der Zugriff auf eine Datei, die vor unberechtigtem Ausführen geschützt ist, erfolgt analog zum Schutzattribut WRITE-PASSWORD.

Schutzattribut DESTROY-BY-DELETE

Durch Setzen des Schutzattributs DESTROY-BY-DELETE kann der Eigentümer angeben, daß beim Löschen einer Datei sowohl der Katalogeintrag gelöscht wird als auch der frei werdende Speicherplatz mit binär Null überschrieben wird.

Schutzattribut AUDIT

Durch das Schutzattribut AUDIT kann der Eigentümer festlegen, daß einzelne Zugriffe auf Objekte durch SAT überwacht werden sollen. Der Operand darf in einem Kommando nur dann verwendet werden, wenn für die Benutzerkennung die entsprechende Berechtigung vorliegt (siehe Seite 55ff).

Schutzattribut RETENTION-PERIOD

Das Schutzattribut RETENTION-PERIOD ermöglicht eine Zeitangabe in Tagen. In dem angegebenen Zeitraum kann eine Datei nur gelesen, jedoch nicht verändert oder gelöscht werden.

6.8 Steuerung des Zugriffsschutzes für die verschiedenen Objekte des BS2000

Schutzattribute für die verschiedenen Objekte des BS2000 können über die Kommando- und die Makroschnittstelle vereinbart werden. Das vorliegende Sicherheitshandbuch behandelt vor allem den Zugriffsschutz über die Kommandoschnittstelle.

6.8.1 Dateien

Über die Kommandoschnittstelle können Schutzattribute für Dateien, Dateigenerationen und Dateigenerationsgruppen vereinbart werden. Diese können auf gemeinschaftlichen Plattenspeichern, privaten Plattenspeichern, Magnetbändern, Magnetbandkassetten oder Disketten abgespeichert sein.

6.8.2 Gemeinschaftliche Plattendateien

Gemeinschaftliche Plattendateien sind Dateien, die auf Plattenspeichern eines Pubset abgelegt sind. Die Plattenspeicher eines Pubset werden auch als gemeinschaftlicher Plattenspeicher bezeichnet. Für jede gemeinschaftliche Plattendatei existiert ein Eintrag im Dateikatalog des entsprechenden Pubset, der alle Attribute der Datei enthält. Gemeinschaftliche Plattendateien können sich über mehrere Plattenspeicher erstrecken, die jedoch dem gleichen Pubset angehören müssen.

Ein Benutzer kann auf Dateien eines Pubset nur dann zugreifen, wenn seine Benutzerkennung von der Benutzerverwaltung durch das Kommando ADD-USER in den Benutzerkatalog des Pubset eingetragen wurde. Bei der Verwendung von Multiple-Public-Volume-Sets (MPVS) kann durch einen Generierungsparameter der Zugriff auf die mehrbenutzbaren Dateien anderer Pubsets des MPVS erlaubt werden, ohne daß der Benutzer in den Benutzerkatalog eines jeden Pubset eingetragen sein muß.

Der einer Benutzerkennung maximal zur Verfügung stehende Speicherplatz auf dem Pubset wird durch den Operanden PUBLIC-SPACE-LIMIT festgesetzt. In Ausnahmefällen kann ein Überschreiten dieses Wertes durch Angabe von PUBLIC-SPACE-EXCESS=YES von der Benutzerverwaltung ermöglicht werden. Über das Kommando SHOW-USER-ATTRIBUTES kann ein Benutzer die aktuelle Belegung der Attribute seiner Benutzerkennung abfragen (siehe Seite 58).

Zu beachten ist insbesondere, daß stets die Benutzergruppenstruktur des Home-Pubset der laufenden BS2000-Sitzung für die Überprüfung der Zugriffsberechtigung herangezogen wird. Benutzergruppenstrukturen auf Daten-Pubsets haben keine Wirkung.

Mit den Kommandos

CREATE-GUARD
MODIFY-GUARD-ATTRIBUTES
COPY-GUARD
DELETE-GUARD

ADD-ACCESS-CONDITIONS
MODIFY-ACCESS-CONDITIONS
REMOVE-ACCESS-CONDITIONS

wird der Zugriffsschutz durch GUARDS geregelt.

Mit den Kommandos

CREATE-FILE-ACL
ADD-FILE-ACL-ENTRY
MODIFY-FILE-ACL-ENTRY
REMOVE-FILE-ACL-ENTRY
DELETE-FILE-ACL (siehe Anhang A)

wird der Zugriffsschutz durch die Zugriffskontrolliste (ACL) geregelt.

Mit den Kommandos

CREATE-FILE und
MODIFY-FILE-ATTRIBUTES (siehe Anhang A)

können die übrigen Schutzmechanismen bzw. Schutzattribute für gemeinschaftliche Plattendateien vereinbart werden. Eine Änderung der Schutzmechanismen und Schutzattribute ist für Plattendateien prinzipiell jederzeit durch den Eigentümer möglich. Wird einer der Operanden beim CREATE-FILE-Kommando nicht angegeben, werden automatisch die Standardwerte übernommen. Wird beim MODIFY-FILE-ATTRIBUTES-Kommando ein Operand nicht angegeben, bleibt der aktuelle Wert unverändert. Die Überprüfung der Zugriffsberechtigung erfolgt bei jeder Dateieröffnung.

Die Anzeige der Schutzmechanismen und Schutzattribute erfolgt durch die Kommandos

für GUARDS:

SHOW-GUARD-ATTRIBUTES
SHOW-ACCESS-ADMISSION
SHOW-ACCESS-CONDITIONS
SHOW-FILE-ATTRIBUTES (siehe Anhang A)

für ACL:

SHOW-FILE-ACL und
SHOW-FILE-ATTRIBUTES (siehe Anhang A).

Folgende Schutzmechanismen bzw. Schutzattribute werden beim Zugriffsschutz für gemeinschaftliche Plattendateien berücksichtigt:

- Guard,
- Zugriffskontrolliste (ACL),
- einfache Zugriffskontrolliste (BASIC-ACL),
- ACCESS,
- USER-ACCESS,
- WRITE-PASSWORD,
- READ-PASSWORD,
- EXEC-PASSWORD,
- DESTROY-BY-DELETE,
- AUDIT,
- RETENTION-PERIOD.

Guard

GUARDS stellt zwei Gruppen von Benutzerkommandos zur Verfügung.

Kommandos zur Verwaltung eines Guard:

CREATE-GUARD richtet ein Guard ein und legt die Attribute fest. Beim Einrichten werden Name, Verwendungsberechtigung (SCOPE-Attribut) und ein Kommentar festgelegt.

COPY-GUARD kopiert ein Guard. Fremde Kennungen dürfen ein Guard nur kopieren, wenn dies durch das SCOPE-Attribut zugelassen ist.

DELETE-GUARD löscht ein Guard. Nur der Eigentümer darf ein Guard löschen.

Kommandos zur Verwaltung der Bedingungen:

ADD-ACCESS-CONDITIONS
definiert Zugriffsbedingungen für die Subjekttypen USER, GROUP, OTHERS und das Pseudosubjekt ALL-USERS. Durch mehrfachen Aufruf können Einträge für verschiedene Subjekttypen gemacht werden. Wird der Name eines nicht existierenden Guards angegeben, so wird ein neues mit dem angegeben Namen erzeugt. Dieses Guard hat die Standardattribute.

MODIFY-ACCESS-CONDITIONS
ändert bestehende Bedingungsdefinitionen.

REMOVE-ACCESS-CONDITIONS
entfernt ein oder mehrere Bedingungsdefinitionen aus einem Guard. Werden alle Bedingungen gelöscht, bleibt das Guard als Objekt erhalten. Wird nun die Bedingungsauswertung aufgerufen, lautet das Ergebnis der Auswertung immer "Bedingung nicht erfüllt".

Der Zugriffsschutz mit Hilfe von GUARDS für eine Datei oder ein Bibliothekselement ist erst aktiv, wenn ein Guard zugewiesen wurde. Wird versucht auf eine Datei oder ein Bibliothekselement zuzugreifen, für das ein Eintrag eines Guards existiert, dieses Guard jedoch nicht verwendet werden kann, gibt GUARDS das Ergebnis "Bedingung nicht erfüllt" zurück. Ein Guard kann nicht verwendet werden, wenn es nicht existiert, das SCOPE-Attribut des Guards die Verwendung durch eine fremde Benutzerkennung nicht zuläßt oder noch keine Zugriffsbedingungen definiert wurden.

Zugriffskontrolliste (ACL)

Das Aktivieren einer ACL erfolgt mit dem Kommando CREATE-FILE-ACL. Dieses Kommando bietet folgende Möglichkeiten:

- Abbildung der zuvor gültigen Schutzmechanismen (die BASIC-ACL oder die Schutzattribute ACCESS und USER-ACCESS, siehe Seite 98) durch Angabe von *PREVIOUS.
- Kopieren eines bereits bestehenden ACL-Eintrags durch Angabe von *FROM.
- Setzen der standardmäßig gültigen Zugriffsrechte (OTHERS-Eintrag) durch Angabe von *OTHERS.

Das Ändern eines ACL-Eintrags erfolgt durch die Kommandos

- ADD-FILE-ACL-ENTRY (Hinzufügen neuer Benutzerkennungen und neuer Gruppenkennungen),
- MODIFY-FILE-ACL-ENTRY (Ändern bereits eingetragener Benutzerkennungen und Gruppenkennungen sowie des OTHERS-Eintrags) und
- REMOVE-FILE-ACL-ENTRY (Löschen von Benutzerkennungen und Gruppenkennungen).

Das Deaktivieren eines ACL-Eintrags erfolgt mit dem Kommando DELETE-FILE-ACL.

Einfache Zugriffskontrolliste (BASIC-ACL)

Das Aktivieren oder Ändern einer BASIC-ACL für eine Datei erfolgt mit den Operanden OWNER, GROUP und OTHERS der Kommandos CREATE-FILE bzw. MODIFY-FILE-ATTRIBUTES.

Das Deaktivieren einer BASIC-ACL erfolgt durch Angabe von MODIFY-FILE-ATTRIBUTES..., BASIC-ACL=NONE.

Bei einer Überprüfung der Zugriffsrechte wird die BASIC-ACL nur dann ausgewertet, wenn sie aktiviert ist, die ACL jedoch nicht. Wird für eine durch die BASIC-ACL geschützte Datei die ACL aktiviert, bleibt die Einstellung der BASIC-ACL erhalten, d.h. bei Deaktivierung der ACL wirkt die BASIC-ACL wie sie zuletzt eingerichtet war.

Schutzattribut ACCESS

Das Vergeben oder Ändern des Schutzattributs ACCESS für eine Datei erfolgt mit dem Operanden ACCESS. Gegebenenfalls benötigte Kennwörter müssen in die Kennworttabelle eingetragen werden.

Bei einer Überprüfung der Zugriffsrechte wird das Schutzattribut ACCESS nur dann ausgewertet, wenn weder ein Guard, die ACL noch die BASIC-ACL aktiviert sind.

Schutzattribut USER-ACCESS

Das Vergeben oder Ändern des Schutzattributs USER-ACCESS für eine Datei erfolgt mit dem Operanden USER-ACCESS. Gegebenenfalls benötigte Kennwörter müssen in die Kennworttabelle eingetragen werden.

Bei einer Überprüfung der Zugriffsrechte wird das Schutzattribut USER-ACCESS nur dann ausgewertet, wenn weder ein Guard, die ACL noch die BASIC-ACL aktiviert sind.

Schutzattribut WRITE-PASSWORD

Das Vereinbaren, Ändern oder Löschen eines Schreibkennworts für eine Datei erfolgt mit dem Operanden WRITE-PASSWORD. Das Schreibkennwort muß explizit vergeben oder gelöscht werden.

Vor einem Schreibzugriff auf eine Datei muß das vereinbarte Schreibkennwort angegeben werden (siehe Seite 125). Mit dem Kommando ADD-PASSWORD kann ein Kennwort in die Kennworttabelle des Auftrags eingetragen werden. Ein dort eingetragenes Kennwort erlaubt den Zugriff auf alle Dateien, die durch dieses Kennwort geschützt werden. Soll der Kennwortschutz wiederhergestellt werden, müssen die nicht mehr benötigten Kennwörter mit dem Kommando REMOVE-PASSWORD explizit aus der Kennworttabelle eines Auftrags entfernt werden. Die Kennworttabelle kann vom Benutzer auch vollständig gelöscht werden; bei Auftragsende wird sie implizit gelöscht.

Dateien, die mit einem Kennwort geschützt sind, können nur dann gelöscht werden, wenn der Schreibzugriff möglich ist.

Schutzattribut READ-PASSWORD

Das Vereinbaren, Ändern oder Löschen eines Lesekennworts für eine Datei erfolgt mit dem Operanden READ-PASSWORD.

Es gelten die gleichen Regeln wie beim Schutzattribut WRITE-PASSWORD.

Schutzattribut EXEC-PASSWORD

Das Vereinbaren, Ändern oder Löschen eines Ausführungskennworts für eine Datei erfolgt mit dem Operanden EXEC-PASSWORD.

Es gelten die gleichen Regeln wie beim Schutzattribut WRITE-PASSWORD.

Schutzattribut DESTROY-BY-DELETE

Das Vergeben oder Ändern des Schutzattributs DESTROY-BY-DELETE erfolgt mit dem Operanden DESTROY-BY-DELETE.

Schutzattribut AUDIT

Das Vergeben oder Ändern des Schutzattributs AUDIT für eine Datei erfolgt mit dem Operanden AUDIT.

Das Schutzattribut AUDIT kann von einem Benutzer für eine Datei nur dann vergeben werden, wenn seine Benutzerkennung dazu berechtigt ist. Die Berechtigung wird einer Benutzerkennung von der Benutzerverwaltung durch die Kommandos ADD-USER oder MODIFIY-USER und der Vergabe des Benutzerrechts FILE-AUDIT erteilt.

Schutzattribut RETENTION-PERIOD

Das Vergeben oder Ändern des Schutzattributs RETENTION-PERIOD erfolgt mit dem Operanden RETENTION-PERIOD durch die Kommandos MODIFY-FILE-ATTRIBUTES bzw. SET-FILE-LINK.

Beispiel

a) Für die Datei file1 soll ein Katalogeintrag erstellt werden. Folgende Schutzmechanismen bzw. Schutzattribute sollen vereinbart werden:

   – die BASIC-ACL soll in folgender Einstellung aktiviert werden:

      – uneingeschränkte Zugriffsrechte für die Benutzerkennung des Eigentümers der Datei,
      – Zugriffsrecht Lesen und Schreiben für die Benutzergruppe auf dem Home-Pubset der laufenden BS2000-Sitzung, der der Eigentümer angehört,
      – keine Zugriffsrechte für Benutzerkennungen außerhalb der eigenen Benutzergruppe,

   – Schreibkennwort 'ida7',
   – Überwachung aller fehlerhaften Zugriffe.

b) Für die Datei file1 soll die ACL aktiviert werden, wobei der bestehende Zugriffsschutz durch die BASIC-ACL in die ACL abgebildet werden soll.

c) In den ACL-Eintrag der Datei file1 soll die Benutzerkennung hannibal mit allen Zugriffsrechten aufgenommen werden.

zu a):

```
create-file file-name=file1,-
            basic-acl=(owner=(read=yes,write=yes,exec=yes),-
            group=(read=yes,write=yes,exec=no),-
            others=no-access),-
            write-password='ida7',-
            audit=failure
```

zu b):

Vor dem Aktivieren der ACL ist der Eintrag des Schreibkennworts 'ida7' in die Kennworttabelle des Auftrags vorzunehmen.

```
add-password password=c'ida7'

create-file-acl file-name=file1,access-rights=*previous
```

zu c):

```
add-file-acl-entry file-name=file1,-
                   access-rights=-user(user-identification=hannibal,-
                                                          read=yes,-
                                                          write=yes,-
                                                          execute=yes)
```

6.8.3 Dateien auf privaten Datenträgern

Private Datenträger sind alle Datenträger außer gemeinschaftlichen Plattenspeichern (z.B. private Plattenspeicher, Magnetbänder etc.). Dateien auf privaten Datenträgern, deren Eintrag im Dateikatalog gelöscht wurde oder die in anderen DV-Systemen erstellt wurden, müssen vor der Verarbeitung mit dem IMPORT-FILE-Kommando katalogisiert werden. Dieser Vorgang wird als 'Importieren' bezeichnet. Analog dazu bedeutet 'Exportieren' das Löschen von Katalogeinträgen für Dateien auf privaten Datenträgern mittels des EXPORT-FILE-Kommandos.

Dateien auf privaten Plattenspeichern oder Magnetbändern können sich über mehrere gleiche Datenträger erstrecken. Der Benutzer muß dafür sorgen, daß alle benötigten Datenträger zu Beginn der Verarbeitung dem Betriebssystem bekannt sind.

Anmerkungen:

– Das durch den Operanden PUBLIC-SPACE-LIMIT der Kommandos ADD-USER bzw. MODIFY-USER festgesetzte Speicherplatzkontingent gilt nur für gemeinschaftliche Plattenspeicher, nicht für private Datenträger.

– Im sicheren Betrieb ist die Verwendung privater Plattenspeicher nicht erlaubt.

Private Plattendateien

Private Plattendateien sind Dateien, die auf privaten Plattenspeichern abgelegt sind. Folgende Schutzmechanismen bzw. Schutzattribute werden beim Zugriffsschutz für private Plattendateien berücksichtigt:

– einfache Zugriffskontrolliste (BASIC-ACL),
– ACCESS,
– USER-ACCESS,
– WRITE-PASSWORD,
– READ-PASSWORD,
– EXEC-PASSWORD,
– DESTROY-BY-DELETE,
– AUDIT,
– RETENTION-PERIOD.

Guard und ACL können zum Schutz von privaten Plattendateien nicht herangezogen werden. Die BASIC-ACL wird dann ausgewertet, wenn sie aktiviert ist. Die Schutzattribute ACCESS und USER-ACCESS werden ausgewertet, wenn die BASIC-ACL deaktiviert ist. Für die übrigen Schutzattribute gelten die gleichen Aussagen wie bei gemeinschaftlichen Plattendateien.

Banddateien

Banddateien sind Dateien, die auf Magnetbändern oder Magnetbandkassetten abgespeichert sind. Eine Banddatei kann sich über mehrere Magnetbänder erstrecken; ebenso können auf einem Magnetband mehrere Dateien abgespeichert werden. Da die Benutzerkommandos für die Verarbeitung von Dateien auf Magnetbändern und Magnetbandkassetten identisch sind, wird hier der Begriff "Magnetband" auch synonym für Magnetbandkassette verwendet.

Eine sichere Bandverarbeitung setzt den Einsatz des Software-Produkts MAREN voraus [8]. MAREN ist ein BS2000-Subsystem und dient zur Verwaltung von Magnetbändern (und Magnetbandkassetten) in BS2000-Rechenzentren. Zur besseren Unterscheidung werden im folgenden Schutzattribute, die über das Subsystem MAREN vereinbar sind, als MAREN-Schutzattribute bezeichnet.

MAREN-Schutzattribute werden in einem eigenen Katalog, dem MAREN-Katalog, geführt. Sie sind jederzeit vom Eigentümer des Magnetbandes oder vom Bandverwalter änderbar. MAREN gewährleistet gleichen Zugriffsschutz für alle Magnetbänder.

Schutzattribute, die über das BS2000 vereinbar sind, können in Kennsätzen auf dem Magnetband hinterlegt sein. Die Anordnung und der Aufbau dieser Kennsätze sind genormt (DIN 66029, DIN 66229). Der Benutzer kann im Kommando SET-FILE-LINK über den Operanden LABEL angeben, ob das Magnetband mit Standardkennsätzen, Nicht-Standardkennsätzen oder ohne Kennsätze aufgebaut ist. Damit wird die Verarbeitung von Magnetbändern ermöglicht, die von den Normen DIN 66029 bzw. DIN 66229 abweichen. Die Schutzattribute sind nur bei Verwendung von Standardkennsätzen voll wirksam. Sie können vereinbart bzw. geändert werden, solange eine Banddatei noch nicht auf ein Magnetband geschrieben wurde, d.h. eine Änderung der Schutzattribute nach dem ersten Eröffnen einer Banddatei ist nicht mehr möglich.

Der Zugriffsschutz für Magnetbänder und Banddateien erstreckt sich über vier Ebenen:

1) Schutz des Magnetbandes durch MAREN,
2) Schutz der Banddatei durch MAREN,
3) Schutz des Magnetbandes durch Bandkennsätze und
4) Schutz der Banddatei durch Dateikennsätze.

Der Zugriff auf ein Magnetband oder eine Banddatei wird nur dann gewährt, wenn sowohl MAREN als auch das BS2000 den Zugriff gestatten.

1) Schutz des Magnetbandes durch MAREN

   Folgende Schutzattribute können für ein Magnetband über MAREN vergeben werden:

   - MAREN-Schutzattribut FREE-DATE,
   - MAREN-Schutzattribut PASSWORD,
   - MAREN-Schutzattribut USER-ACCESS.

   MAREN-Schutzattribut FREE-DATE

   Das Vergeben oder Ändern des MAREN-Schutzattributs FREE-DATE erfolgt mit dem Operanden FREE-DATE der MAREN-Kommandos MODIFY-VOLUME-ATTRIBUTES bzw. RESERVE-FREE-VOLUME.

   Das MAREN-Schutzattribut FREE-DATE bestimmt ein Datenträger-Freigabedatum. Bis zu diesem Datum bleibt das Magnetband für den eingetragenen Besitzer (=Eigentümer) reserviert. Während dieser Zeit kann der Eigentümer das Magnetband beliebig oft lesen, neu beschreiben, ausleihen etc. Im MAREN-Katalog wird auch das Datei-Freigabedatum (siehe unter (2): MAREN-Schutzattribut EXPIRATION-DATE) eingetragen. Das MAREN-Subsystem sorgt intern dafür, daß das Datenträger-Freigabedatum mindestens so hoch ist, wie das Datei-Freigabedatum.

MAREN-Schutzattribut PASSWORD

Das Vergeben des MAREN-Schutzattributs PASSWORD erfolgt mit dem Operanden PASSWORD des MAREN-Kommandos RESERVE-FREE-VOLUME bzw. mit dem Operanden NEW-PASSWORD des MAREN-Kommandos MODIFY-VOLUME-ATTRIBUTES. Das Ändern des Schutzattributs PASSWORD erfolgt mit dem Operanden NEW-PASSWORD des MODIFY-VOLUME-ATTRIBUTES-Kommandos, wobei das aktuelle Kennwort mit dem Operanden PASSWORD angegeben werden muß. Durch Setzen des MAREN-Schutzattributs PASSWORD kann der Eigentümer ein Kennwort zum Schutz vor unberechtigtem Zugriff auf das Magnetband festlegen. Bei Zugriff auf das Magnetband muß in den entsprechenden MAREN-Kommandos das Kennwort angegeben werden. Ein Eintrag des Kennworts in die Kennworttabelle des Auftrags ist nicht erforderlich.

MAREN-Schutzattribut USER-ACCESS

Das Vergeben oder Ändern des MAREN-Schutzattributs USER-ACCESS erfolgt mit dem Operanden USER-ACCESS der MAREN-Kommandos MODIFY-VOLUME-ATTRIBUTES bzw. RESERVE-FREE-VOLUME.

Durch das MAREN-Schutzattribut USER-ACCESS kann der Zugriff auf ein Magnetband eingeschränkt werden:

USER-ACCESS=OWNER-ONLY
Der Zugriff auf das Magnetband ist nur dem Eigentümer vorbehalten.

USER-ACCESS=FOREIGN-READ-ONLY
Für Benutzerkennungen ungleich der des Eigentümers ist nur lesender Zugriff auf das Magnetband erlaubt.

USER-ACCESS=ALL-USERS
Alle Benutzerkennungen können auf das Magnetband zugreifen.

2) Schutz der Banddatei durch MAREN

Folgendes Schutzattribut kann für eine Banddatei über MAREN vergeben werden:

MAREN-Schutzattribut EXPIRATION-DATE

Das Ändern des MAREN-Schutzattributs EXPIRATION-DATE erfolgt mit dem Operanden EXPIRATION-DATE des MAREN-Kommandos MODIFY-VOLUME-ATTRIBUTES.

Das MAREN-Schutzattribut EXPIRATION-DATE bestimmt das Datei-Freigabedatum. Bei der Erstellung einer Banddatei wird der Wert des Schutzattributs RETENTION-PERIOD (siehe unter 4)): Schutzattribut RETENTION-PERIOD) in den MAREN-Katalog übernommen. Bis zum Datei-Freigabedatum kann die Banddatei nicht überschrieben werden.

3) Schutz des Magnetbandes durch Bandkennsätze

   Folgendes Schutzattribut kann für ein Magnetband vom BS2000 vergeben werden:

   Schutzattribut Bandeigentümer

   Über das Dienstprogramm INIT kann von der Systembedienung ein Bandeigentümer bestimmt und in einen Bandkennsatz eingetragen werden.

   Die Benutzung eines Magnetbandes ist ausschließlich dem Bandeigentümer vorbehalten, wenn der Dateieigentümer der ersten Banddatei identisch mit dem Bandeigentümer ist und wenn für die erste Banddatei USER-ACCESS=OWNER-ONLY gilt (siehe unter 4)): Schutzattribut USER-ACCESS).

4) Schutz der Banddatei durch Dateikennsätze

   Folgende Schutzmechanismen bzw. Schutzattribute können für eine Banddatei vom BS2000 vergeben werden:

   - ACCESS,
   - USER-ACCESS,
   - WRITE-PASSWORD
   - READ-PASSWORD,
   - EXEC-PASSWORD,
   - DESTROY-BY-DELETE,
   - AUDIT,
   - RETENTION-PERIOD,
   - Dateiname.

   Anmerkung:

   Weder ein Guard, noch die ACL, noch die BASIC-ACL kann zum Schutz von Banddateien herangezogen werden.

   Schutzattribut ACCESS

   Das Vergeben oder Ändern des Schutzattributs ACCESS erfolgt analog zu Plattendateien.

   Schutzattribut USER-ACCESS

   Das Vergeben oder Ändern des Schutzattributs USER-ACCESS erfolgt analog zu Plattendateien. Standardmäßig wird jedoch der Zugriff als mehrbenutzbar vereinbart.

Schutzattribute WRITE-PASSWORD, READ-PASSWORD und EXEC-PASSWORD

Das Vereinbaren, Ändern oder Löschen der Schutzattribute WRITE-PASSWORD, READ-PASSWORD und EXEC-PASSWORD erfolgt analog zu Plattendateien. Eine Überprüfung der Kennwörter erfolgt jedoch nur bei Eingabedateien.

Schutzattribut DESTROY-BY-DELETE

Das Vergeben oder Ändern des Schutzattributs DESTROY-BY-DELETE erfolgt analog zu Plattendateien. Beim Löschen der Banddatei werden auch eventuell folgende Banddateien auf dem Magnetband mit binären Nullen überschrieben.

Schutzattribut AUDIT

Das Vergeben oder Ändern des Schutzattributs AUDIT erfolgt analog zu Plattendateien.

Schutzattribut RETENTION-PERIOD

Das Vergeben oder Ändern des Schutzattributs RETENTION-PERIOD erfolgt durch das Kommando SET-FILE-LINK.

Schutzattribut Dateiname

Das Vergeben oder Ändern des Dateinamens erfolgt analog zu Plattendateien. Das BS2000 überprüft den vom Benutzer angegeben und den in den Dateikennsätzen abgespeicherten Dateinamen auf Übereinstimmung.

Prüfung der Kennsätze

Die Bandkennsätze werden nach dem Montieren des Magnetbandes beim ersten Eröffnen einer Banddatei geprüft. Die Dateikennsätze werden bei jedem Eröffnen einer Banddatei geprüft. Die Kennsatzprüfung kann nur mit einer besonderen Berechtigung umgangen werden (s. unten). Werden bei der Kennsatzprüfung Fehler erkannt, wird die Prüfung unterbrochen und eine Fehlermeldung ausgegeben. Fehlermeldungen, die Dateikennsätze oder die Zugriffsberechtigung auf das Magnetband betreffen, werden an der Datensichtstation des Benutzers ausgegeben, alle übrigen an einer Bedienstation der Systembedienung. Der Meldungstext erläutert, wie auf die jeweilige Fehlermeldung reagiert werden kann.

Einige der Fehlermeldungen können durch "Ignorieren" vernachlässigt werden. Welche Fehlermeldungen ignoriert werden können, hängt davon ab, ob die Benutzerkennung des laufenden Auftrags auch der Dateieigentümer ist bzw. mit welchen Rechten die Benutzerkennung des laufenden Auftrags ausgestattet ist:

- Der Dateieigentümer kann seine Banddatei betreffende Fehlermeldungen ignorieren.
- Die Ausprägungen des Benutzerrechts TAPE-ACCESS bedeuten (siehe Seite 55):
  - TAPE-ACCESS=STD
    Der Benutzer darf keine Fehlermeldungen ignorieren.
  - TAPE-ACCESS=READ
    Der Benutzer darf Fehlermeldungen ignorieren, die sich auf Eingabedateien beziehen.
  - TAPE-ACCESS=BYPASS-LABEL
    Der Benutzer darf die Kennsatzprüfung bei Eingabedateien umgehen.
  - TAPE-ACCESS=PRIVILEGED
    Der Benutzer darf Fehlermeldungen ignorieren.
  - TAPE-ACCESS=ALL
    Der Benutzer darf Kennsatzprüfungen umgehen und Fehlermeldungen ignorieren.
- Die Berechtigung der Systemverwaltung entspricht der von TAPE-ACCESS=ALL.

Fehlermeldungen, die aus einer Verletzung von Schutzattributen resultieren, werden wie folgt behandelt:

- Fehlermeldung wegen unerlaubten Zugriffs auf eine nicht mehrbenutzbare Banddatei (Schutzattribut USER-ACCESS).

  Die Fehlermeldung kann nicht ignoriert werden; der Zugriff wird abgewiesen.
- Fehlermeldung wegen schreibenden Zugriffs auf eine Banddatei, für die nur lesender Zugriff erlaubt ist (Schutzattribute ACCESS, RETENTION-PERIOD).

  Die Fehlermeldung kann ignoriert werden von:

  - dem Dateieigentümer,
  - Benutzerkennungen mit TAPE-ACCESS=PRIVILEGED,
  - Benutzerkennungen mit TAPE-ACCESS=ALL,
  - der Systemverwaltung.
- Fehlermeldung wegen nicht übereinstimmenden Dateinamens (Schutzattribut Dateiname).

Die Fehlermeldung kann ignoriert werden von:

- dem Dateieigentümer,
- Benutzerkennungen mit TAPE-ACCESS=READ,
- Benutzerkennungen mit TAPE-ACCESS=BYPASS-LABEL,
- Benutzerkennungen mit TAPE-ACCESS=PRIVILEGED,
- Benutzerkennungen mit TAPE-ACCESS=ALL,
- der Systemverwaltung.

- Fehlermeldung wegen unerlaubten Zugriffs auf ein nur vom Bandeigentümer benutzbares Magnetband (Schutzattribut Bandeigentümer).

  Die Fehlermeldung kann nicht ignoriert werden; der Zugriff wird abgewiesen.

Implizites Löschen

Bei schreibendem Zugriff auf eine Banddatei werden alle auf diesem Magnetband vorher vorhandenen Banddateien unabhängig von deren Schutzattributen implizit gelöscht. Die Katalogeinträge bleiben zwar erhalten, auf die Daten kann jedoch nicht mehr zugegriffen werden. Dies ist bei jedem schreibendem Zugriff auf Magnetbänder zu beachten.

Das BS2000 bietet eine wirkungsvolle Maßnahme, um implizitem Löschen vorzubeugen:

Wird beim Kommando SET-FILE-LINK der Operand OVERWRITE-PROTECTION=YES angegeben, überprüft das BS2000 bei schreibendem Zugriff die Schutzattribute ACCESS und RETENTION-PERIOD, wenn die aktuelle Banddatei nicht als erste Banddatei auf dem Magnetband abgespeichert wird.

Das Beschreiben des Magnetbandes wird abgewiesen, wenn:

- für die aktuelle Banddatei ACCESS=READ vereinbart wurde, für die unmittelbar davor abgespeicherte Banddatei ACCESS=WRITE gilt, oder
- das Freigabedatum der aktuellen Banddatei höher ist als das der unmittelbar davor abgespeicherten Banddatei.

Empfehlungen zur Verwendung von Banddateien

- Bei Magnetbändern mit Standardkennsätzen soll beim Kommando SET-FILE-LINK der Operand LABEL in einer der folgenden drei Einstellungen angegeben werden:

  ```
  LABEL=STD(DIN-REVISION-NUMBER=HIGHEST),
  LABEL=STD(DIN-REVISION-NUMBER=3) oder
  LABEL=STD(DIN-REVISION-NUMBER=2).
  ```

- Banddateien sind automatisch so gut geschützt, wie das Magnetband selbst. Deshalb soll besonderer Wert auf den Schutz des Magnetbandes gelegt werden.

– Die in den Kennsätzen abgespeicherten Schutzmechanismen und Schutzattribute werden beim Importieren von Banddateien in den Katalogeintrag übernommen. Anschließend können diese Dateien z.B. durch ein Guard oder die ACL zusätzlich geschützt werden.

6.8.4 Dateigenerationen

Eine Dateigenerationsgruppe ist eine Menge von katalogisierten Dateien (= Dateigenerationen) mit gleichen Eigenschaften. Innerhalb der Dateigenerationsgruppe werden die Dateigenerationen über ihre Generationsnummer eindeutig identifiziert.

Für Dateigenerationen kann kein Zugriffsschutz durch die Zugriffskontrolliste (ACL) oder Guards vereinbart werden.

Die übrigen Schutzmechanismen und Schutzattribute (Ausnahme: BASIC-ACL) werden für alle Dateigenerationen einer Dateigenerationsgruppe mit den Kommandos CREATE-FILE-GROUP bzw. MODIFY-FILE-GROUP-ATTRIBUTES vergeben. Sie werden im Eintrag der Dateigenerationsgruppe und im Eintrag der einzelnen Dateigenerationen hinterlegt.

Analog zu Dateien können folgende Schutzmechanismen bzw. Schutzattribute vergeben werden:

– ACCESS,
– USER-ACCESS,
– WRITE-PASSWORD,
– READ-PASSWORD,
– DESTROY-BY-DELETE,
– AUDIT,
– RETENTION-PERIOD.

Das Schutzattribut EXEC-PASSWORD kann für Dateigenerationen nicht vergeben werden, da Dateigenerationen keine ausführbaren Dateien (Prozedur- oder Programmdateien) sein können.

Darüber hinaus können weitere sicherheitsrelevante Merkmale festgelegt werden:

OVERFLOW-OPTION

Über den Operanden OVERFLOW-OPTION wird gesteuert, was geschehen soll, wenn die maximal erlaubte Anzahl von Dateigenerationen überschritten wird. Möglich ist ein zyklisches Überschreiben der Dateigenerationen oder ein Löschen aller Dateigenerationen.

BASE-NUMBER

Über den Operanden BASE-NUMBER wird der Basiswert einer Dateigenerationsgruppe festgelegt. Auf diesen Wert beziehen sich alle relativen Generationsnummern. Die Art des Datenträgers, auf dem die Dateigenerationen abgespeichert sind, wird mit den Kommandos CREATE-FILE-GENERATION bzw. MODIFY-FILE-GENERATION-SUPPORT festgelegt (Operand SUPPORT). Dateigenerationsgruppen können auf gemeinschaftlichen oder privaten Datenträgern erstellt und verarbeitet werden. Eine gemischte Verwendung von gemeinschaftlichen Plattenspeichern und Magnetbändern ist dabei möglich.

Bei der Reservierung von Betriebsmitteln mit dem Kommando SECURE-RESOURCE-ALLOCATION ist zu beachten, daß bei exklusiver Reservierung einer Dateigenerationsgruppe alle Dateigenerationen gegen fremden Zugriff gesperrt werden.

Eine umfassende Beschreibung von Dateigenerationen und Dateigenerationsgruppen findet sich im Handbuch "BS2000-DVS Einführung und Kommandoschnittstelle" [10].

6.8.5 Auswirkungen der Vergabe von Schutzmechanismen bzw. Schutzattributen auf Benutzerkommandos

Bei der Vergabe von Schutzmechanismen bzw. Schutzattributen sind die Auswirkungen auf folgende Kommandos zu beachten:

ASSIGN-SYSDTA
ASSIGN-SYSIPT
ASSIGN-SYSLST
ASSIGN-SYSOPT
ASSIGN-SYSOUT

Der Zugriff (lesender Zugriff bei SYSDTA und SYSIPT; schreibender Zugriff bei SYSLST, SYSOPT und SYSOUT) auf eine zugewiesene Datei muß möglich sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle des Auftrags eingetragen werden. Die Datei darf nicht gesperrt sein (z.B. durch einen anderen Auftrag belegt).

COPY-FILE

Sendedatei:

Es muß Lesezugriff auf die Datei möglich sein und die Datei darf nicht gesperrt sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle eingetragen werden.

Empfangsdatei:

Ist die Datei bereits katalogisiert, so muß Schreibzugriff auf die Datei möglich sein und die Datei darf nicht gesperrt sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle eingetragen werden.

Ein ACL-Eintrag bzw. die BASIC-ACL werden nur dann übernommen, wenn

- die Sende- und die Empfangsdatei den gleichen Eigentümer besitzen,
- die Sende- und die Empfangsdatei die gleiche Katalogkennung besitzen und
- die Empfangsdatei eine gemeinschaftliche Plattendatei ist.

Die übrigen Schutzattribute der Sendedatei werden übernommen, wenn der Operand PROTECTION=SAME angegeben wird, ansonsten werden Standardwerte gesetzt.

DELETE-FILE
DELETE-FILE-GENERATION
DELETE-FILE-GROUP
EXPORT-FILE

Nur der Dateieigentümer kann löschen. Es muß Schreibzugriff auf die entsprechende Datei, Dateigeneration bzw. Dateigenerationsgruppe möglich sein und die Datei darf nicht gesperrt sein. Ein eventuell benötigtes Kennwort kann im Kommando angegeben und braucht nicht in die Kennworttabelle eingetragen zu werden (Operand PASSWORDS-TO-IGNORE). Ebenso kann der Dateieigentümer ein Guard, die ACL, die BASIC-ACL und die Schutzattribute USER-ACCESS und RETENTION-PERIOD ignorieren, ohne den Katalogeintrag der Datei ändern zu müssen (Operand IGNORE-PROTECTION). Wird die Datei bzw. die Dateigenerationsgruppe durch ein Guard oder die ACL geschützt, wird auch der Verweis auf den Schutzmechanismus gelöscht.

CALL-PROCEDURE
ENTER-JOB
LOAD-PROGRAM
RESTART-PROGRAM
START-PROGRAM

Es muß Ausführungszugriff auf die Datei möglich sein und die Datei darf zum Zeitpunkt des ENTER-, LOAD- oder START-Kommandos nicht gesperrt sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle eingetragen werden. Während der Unterbrechung des Programms bzw. der Prozedur bleibt die Datei gesperrt. Ihre Attribute können nicht geändert werden. Das Zugriffsrecht bleibt erhalten, auch wenn während der Unterbrechung Kennwörter aus der Kennwortliste ausgetragen werden.

MODIFY-FILE-ATTRIBUTES
MODIFY-GENERATION-SUPPORT
MODIFY-FILE-GROUP-ATTRIBUTES

Nur der Eigentümer kann die Attribute der Datei bzw. Dateigenerationsgruppe ändern. Die Datei darf nicht gesperrt sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle eingetragen werden. Für Plattendateien gilt ferner: Gilt für die Datei bzw. Dateigenerationsgruppe DESTROY-BY-DELETE=YES, so wird bei Verwendung des Operanden SPACE=RELEASE freiwerdender Speicherplatz bis zur letzten belegten Seite binär Null überschrieben.

PRINT-FILE

Es muß Lesezugriff auf die Datei möglich sein und die Datei darf nicht gesperrt sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle eingetragen werden. Wird der Operand DELETE-FILE=YES oder DELETE-FILE=DESTROY verwendet, muß Schreibzugriff auf die Datei möglich sein.

SHOW-FILE

Es muß Lesezugriff auf die Datei möglich sein und die Datei darf nicht gesperrt sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle eingetragen werden.

REPAIR-DISK-FILES

Es muß Schreibzugriff auf die Datei möglich sein. Ein evtl. benötigtes Kennwort muß zuvor in die Kennworttabelle eingetragen werden. Durch das Kommando wird eine evtl. vorhandene Dateisperre aufgehoben.

SECURE-RESOURCE-ALLOCATION

Eine Datei eines fremden Benutzers kann nur reserviert werden, wenn über ein Guard, die ACL, die BASIC-ACL bzw. das Schutzattribut USER-ACCESS der Zugriff erlaubt ist.

SET-FILE-LINK

Dateien fremder Benutzer können nur dann zugewiesen werden, wenn über ein Guard, die ACL, die BASIC-ACL bzw. das Schutzattribut USER-ACCESS der Zugriff erlaubt ist.

6.8.6 Jobvariablen

Jobvariablen sind Speicherbereiche zum Austausch von Informationen zwischen Aufträgen untereinander sowie zwischen dem Betriebssystem und Aufträgen. Es gibt zwei Arten von Jobvariablen:

- Benutzer-Jobvariablen und
- Sonder-Jobvariablen.

Benutzer-Jobvariablen

Sie werden vom Benutzer mit dem Kommando CREATE-JV erzeugt und katalogisiert. Eine katalogisierte Jobvariable existiert solange, bis sie explizit mit dem Kommando DELETE-JV gelöscht wird (siehe Seite 157).

Mit den Kommandos CREATE-JV bzw. MODIFY-JV-ATTRIBUTES können folgende Schutzmechanismen bzw. Schutzattribute vereinbart werden (analog zu denen für Dateien):

- einfache Zugriffskontrolliste (BASIC-ACL),
- ACCESS,
- USER-ACCESS,
- WRITE-PASSWORD,
- READ-PASSWORD,
- RETENTION-PERIOD,
- MONJV-PROTECTION (falls die Jobvariable zur Auftragsüberwachung eingesetzt werden soll).

Mit dem Kommando MODIFY-JV kann der Benutzer einer Jobvariablen einen Wert zuweisen (Operand VALUE). Dabei kann ein evtl. vorhandener Wert ganz oder teilweise durch den neuen Wert ersetzt werden (Operanden POSITION und LENGTH). In Abhängigkeit des Wertes einer Jobvariablen kann mit dem Kommando MODIFY-JV-CONDITIONALLY der Wert der Jobvariablen geändert werden (Operanden IF-VALUE und SET-VALUE). In dem Zeitintervall, in dem der Wert der Jobvariablen überprüft und ggfs. geändert wird, ist die Jobvariable für andere Aufträge nicht zugreifbar.

Wird eine Jobvariable zur Auftragsüberwachung eingesetzt, so ist folgendes zu beachten:

- Die Überprüfung der Zugriffsberechtigung erfolgt stets gegenüber dem Home-Pubset der laufenden BS2000-Sitzung.

- Kennwörter für Jobvariablen müssen dem Betriebssystem vor dem ersten Zugriff bekannt sein. Änderungen der Schutzattribute während eines Auftrags haben keinen Einfluß auf die Verfügbarkeit der Jobvariablen für den laufenden Auftrag. Nur die Änderung der Mehrbenutzbarkeit (Operand USER-ACCESS) wird sofort erkannt.
- Das Betriebssystem schützt die ersten 128 Byte einer auftragsüberwachenden Jobvariablen vor Schreibzugriff. Dieser Schutz beginnt bei Auftragsbeginn und wird bei Auftragsende des überwachten Auftrags wieder aufgehoben. Ist die Freigabe nicht möglich, bleibt die Jobvariable bis zum nächsten Systemstart oder bis zur expliziten Freigabe durch den Benutzer (durch das Kommando MODIFY-JV-ATTRIBUTES..., MONJV-PROTECTION=NO) gesperrt. Während der Schutzdauer kann die Jobvariable keinem anderen Auftrag oder Programm als überwachende Jobvariable zugewiesen werden.

Sonder-Jobvariablen

Sie werden vom Betriebssystem zur Verfügung gestellt, um den Zugriff auf bestimmte Systeminformationen zu ermöglichen. Ein Teil der Sonder-Jobvariablen enthält allgemeine Informationen (z.B. Uhrzeit), ein anderer Teil auftragsspezifische Informationen (z.B. Benutzerkennung der laufenden Task). Diese Informationen sind nur dem jeweiligen Auftrag zugänglich, d.h. auftragsspezifische Informationen fremder Aufträge, auch solcher unter gleicher Benutzerkennung, können über Sonder-Jobvariablen nicht abgefragt werden.

Sonder-Jobvariablen sind über die Pseudo-Benutzerkennung SYSJV zu erreichen. Eine Benutzerkennung SYSJV darf daher nicht neu eingerichtet werden. Der Zugriff auf die Sonder-Jobvariablen ist nur im Lesemodus erlaubt und wird mit den Kommandos SHOW-JV oder SKIP-COMMANDS (Operand JV) durchgeführt.

Eine ausführliche Beschreibung der Jobvariablen findet sich im Handbuch "BS2000 - JV Jobvariablen Beschreibung" [15].

6.8.7 Benutzerschalter

Jedem Benutzer stehen unter seiner Benutzerkennung 32 Benutzerschalter zur Verfügung. Sie können die Werte 0 (= nicht gesetzt) oder 1 (= gesetzt) annehmen. Die Schalterstellung kann zur Steuerung von Prozeduren ausgewertet werden. Beim Zugriff auf Benutzerschalter ist folgendes zu beachten:

- Jeder Auftrag, der unter einer Benutzerkennung läuft, kann die Schalterstellung eines Benutzerschalters ändern. Dazu steht das Kommando MODIFY-USER-SWITCHES zur Verfügung. Aufträge unter fremden Benutzerkennungen können die Benutzerschalter nicht verändern.

- Über das Kommando SHOW-USER-SWITCHES kann die Schalterstellung von Benutzerschaltern abgefragt werden. Die Schalterstellungen fremder Benutzerkennungen können ebenfalls abgefragt werden (Operand USER-IDENTIFICATION).
- Mit dem Kommando SKIP-COMMANDS kann die Schalterstellung der Benutzerschalter zur Prozedursteuerung ausgewertet werden (Operand USER-SWITCHES). Die Benutzerschalter fremder Benutzerkennungen können ebenfalls ausgewertet werden (Operand USER-IDENTIFICATION).

Die Stellung von Benutzerschaltern bleibt über das Auftragsende hinaus erhalten.

6.8.8 Auftragsschalter

Jedem Auftrag stehen 32 Auftragsschalter zur Verfügung. Sie können die Werte 0 (= nicht gesetzt) oder 1 (= gesetzt) annehmen. Die Schalterstellung kann zur Programm- oder Prozedursteuerung ausgewertet werden. Beim Zugriff auf Auftragsschalter ist folgendes zu beachten:

- Die Auftragsschalter sind an einen Auftrag gebunden. Sie können nur von diesem Auftrag gelesen, verändert oder ausgewertet werden. Dazu stehen die Kommandos MODIFY-JOB-SWITCHES SHOW-JOB-SWITCHES und SKIP-COMMANDS (Operand JOB-SWITCHES) zur Verfügung.
- Das Kommando SET-JOB-STEP setzt die Auftragsschalter 16 bis 31 auf den Wert 0 zurück.
- Alle Auftragsschalter werden bei Auftragsbeginn auf Null gesetzt.

6.8.9 Volumes

Der Zugriffsschutz auf Volume-Ebene ist vom jeweiligen Datenträger abhängig. Es sind folgende Datenträger zu unterscheiden:

Gemeinschaftliche Plattenspeicher eines Pubset

Ein Benutzer kann nur dann Datenobjekte auf einem Pubset ablegen und verarbeiten, wenn mit dem Kommando ADD-USER seine Benutzerkennung in den Benutzerkatalog des Pubset eingetragen wurde (Operand PUBLIC-VOLUME-SET). Für jeden Pubset muß ein eigenes ADD-USER-Kommando abgesetzt werden. Auf diesen Pubsets kann er auch auf mehrbenutzbare Dateien anderer Benutzer zugreifen.

Bei der Verwendung von Multiple-Public-Volume-Sets (MPVS) kann durch einen Generierungsparameter der Zugriff auf die mehrbenutzbaren Dateien anderer Pubsets des MPVS erlaubt werden, ohne daß der Benutzer in den Benutzerkatalog eines jeden Pubset eingetragen sein muß.

Private Plattenspeicher

Private Plattenspeicher werden durch eine Archivnummer (VSN) identifiziert. Der Benutzer kann mit dem Kommando SECURE-RESOURCE-ALLOCATION unter Angabe der VSN private Plattenspeicher mehrbenutzbar oder exklusiv reservieren. Auf exklusiv reservierte Datenträger können andere Benutzer bis zur Freigabe nicht zugreifen.

Magnetbänder (und Magnetbandkassetten)

Magnetbänder werden durch das Subsystem MAREN [8] und durch das BS2000 geschützt. Der Zugriff wird nur bei Erlaubnis von MAREN und BS2000 gestattet.

MAREN bietet für alle Magnetbänder (mit Standardkennsätzen, mit Nicht-Standardkennsätzen und ohne Kennsätze) Zugriffsschutz durch die MAREN-Schutzattribute FREE-DATE, PASSWORD und USER-ACCESS (siehe Seite 136ff).

Neben einem mechanischen Schreibschutz unterstützt das BS2000 für Magnetbänder weitere Zugriffsschutzmechanismen. Voraussetzung ist, daß Standardkennsätze verwendet werden und die Benutzerkennung nicht berechtigt ist, Fehlermeldungen bei der Überprüfung der Kennsätze zu ignorieren (Kommando ADD-USER bzw. MODIFY-USER, Operand TAPE-ACCESS). Ferner wird dieser Zugriffsschutz nicht von Dienstprogrammen, wie z.B. PERCON [19], unterstützt. Die Bandkennsätze eines Magnetbandes enthalten das Bandkennzeichen (VSN), ein evtl. vergebenes Eigentümerkennzeichen und den Zugriffsvermerk. Bei Zugriff auf das Magnetband muß die VSN angegeben werden, Eigentümerkennzeichen und Zugriffsvermerk werden überprüft (siehe Seite 136ff).

Der Benutzer kann mit dem Kommando SECURE-RESOURCE-ALLOCATION unter Angabe der VSN Magnetbänder reservieren. Die Reservierung erfolgt immer exklusiv, d.h. das angeforderte Magnetband ist für andere Benutzer bis zur Freigabe gesperrt.

Disketten

Disketten werden durch eine Archivnummer (VSN) identifiziert. Mit Hilfe des Dienstprogramms FDEXIM können Dateien von Magnetplatte auf Disketten geschrieben bzw. Dateien von Disketten auf gemeinschaftliche Magnetplatten eingelesen werden. Beim Beschreiben kann der Benutzer ein Eigentümerkennzeichen (Operand OWNERID) oder Angaben zum Zugriffsschutz wie Lesekennwort (Operand SVPASS) und Schreibschutz (Operand WRPROTECT) im Datenträgerkennsatz einer Diskette vermerken. Beim Zugriff auf eine Diskette wird der Datenträgerkennsatz überprüft. Darüber hinaus ermöglicht das Kommando PUNCH die Vereinbarung weiterer Schutzattribute: die Festlegung einer Zugriffssperre für eine Datei und damit des gesamten Datenträgers (Operand ACCESS), die Einschränkung der Mehrfachbenutzbarkeit durch Überlesen (Operand BYPASS) und das Setzen einer Schutzfrist (Operand RETPD).

Die Verarbeitung von Disketten erfolgt über das Subsystem SPOOL [20] und wird im weiteren. durch die Systemverwaltung bzw. die Systembedienung gesteuert.

Da Disketten auf externen Geräten beliebig weiterverarbeitet werden können, ist die Wirksamkeit der vorhandenen Schutzattribute begrenzt. Es wird deshalb empfohlen, sensitive Daten nicht auf diese Datenträger auszulagern.

6.8.10 Speicherseiten des Adreßraums

Auf den Inhalt von Speicherseiten des virtuellen Adreßraums kann über Speicherabzüge (Dumps) oder Diagnoseprogramme zugegriffen werden.

Speicherabzüge des Adreßraums werden in Dateien gespeichert, die entweder unter der gleichen Benutzerkennung katalogisiert sind, wenn die Auftragsbeschreibung oder das Programm durch keine Schutzattribute geschützt war, oder die unter der Benutzerkennung SYSUSER katalogisiert sind, wenn die Auftragsbeschreibung oder das Programm vor Lesen geschützt war und der Auftrag nur das Ausführungsrecht, nicht aber das Leserecht für dieses Programm hatte. Diese Diagnoseunterlagen können in der Regel nur für den Eigentümer der Auftragsbeschreibung oder des Programms auf Anfrage über die Systemverwaltung zur Verfügung gestellt werden.

Der Benutzer kann Speicherseiten des Adreßraums als geheime Seiten (Secret Pages) kennzeichnen (CSTAT-Makro, Operand PROTECT). In Abhängigkeit von Generierungsoptionen des Betriebssystems werden diese Seiten bei einem Speicherabzug nicht in die Diagnoseunterlagen aufgenommen. Bezüglich Benutzer-Dumps kann festgelegt werden, ob alle oder keine der als geheim gekennzeichneten Seiten in einen Speicherabzug aufgenommen werden sollen.

Werden keine Seiten in den Speicherabzug aufgenommen, müssen Fehler, zu deren Diagnose Information aus den geheimen Seiten notwendig ist, auf einer Anlage reproduziert werden, die einen geringeren Grad an Schutzwürdigkeit bezüglich geheimer Seiten hat.

Speicherabzüge des Systemadreßraums werden grundsätzlich in Dateien unter Benutzerkennungen der Systemverwaltung gespeichert. Sie sind somit für den Benutzer im Teilnehmerbetrieb nicht zugänglich (siehe Sicherheitshandbuch für die Systemverwaltung des BS2000 [12]).

Testprogramme verfügen über ein Schutzstufensystem. Der Ablauf dieser Programme wird benutzerspezifisch durch den Wert des Operanden TEST-OPTIONS gesteuert, den die Benutzerverwaltung beim Einrichten oder Ändern einer Benutzerkennung mit dem Kommando ADD-USER oder MODIFY-USER zuweist.

Die angegebenen Werte für die Lese- und Schreibrechte dürfen die bei der Systemgenerierung festgelegten Werte nicht überschreiten.

6.8.11 Memory-Pools

Über Memory-Pools kann ein zusammenhängender Speicherbereich im Benutzeradreßraum zur Verfügung gestellt werden, der von mehreren Benutzern gemeinsam benutzt werden kann.

Beim Einrichten eines Memory-Pool legt ein Benutzer u.a. dessen Namen und seinen Geltungsbereich fest. Der Name des Memory-Pool wird in einem zentral verwalteten Namenskatalog hinterlegt. Dieser Katalog ist lediglich dem Betriebssystem zugänglich.

Der Geltungsbereich legt fest, ob

- nur die laufende Task (Geltungsbereich LOCAL),
- alle Tasks der Benutzerkennung (Geltungsbereich GROUP),
- alle Tasks der Benutzergruppe (Geltungsbereich USER-GROUP) des OWNER, festgelegt auf dem Home-Pubset der laufenden BS2000-Sitzung, oder
- alle Tasks des Betriebssystems (Geltungsbereich GLOBAL)

sich an den Memory-Pool anschließen dürfen. Damit wird sichergestellt, daß nur berechtigte Benutzer auf Speicherseiten des Memory-Pool zugreifen können.

Die Lebensdauer eines Memory-Pool beginnt, wenn sich der erste Benutzer an ihn anschließt und ihn somit einrichtet. Sie endet, wenn der letzte Benutzer sich vom Memory-Pool abkoppelt. Die Speicherseiten werden freigegeben. Bei erneuter Zuweisung werden die Seiten gelöscht (analog zu den Speicherseiten, die einer Benutzer-Task zugewiesen wurden).

Ist der Benutzer berechtigt, den CSTMP-Makro zu verwenden (Kommando ADD-USER bzw. MODIFY-USER, Operand CSTMP-MACRO-ALLOWED), so kann er die Seiten des Memory-Pool gegen Überschreiben schützen.

Der Zugriff mehrerer Benutzer auf einen Memory-Pool kann über Serialisierung (Seite 155) oder Ereignissteuerung (Eventing, Seite 156) koordiniert werden. Analog zum Memory-Pool werden diese ebenfalls (neben Schreibzugriff) durch einen Namen und einen Geltungsbereich definiert. So wird sichergestellt, daß nur Benutzer, die den Namen kennen und aus dem zugehörigen Geltungsbereich stammen, an der Ereignissteuerung teilnehmen können. (Bezüglich weitergehender Informationen siehe Handbuch "BS2000-Makroaufrufe an den Ablaufteil" [16]).

Eine Sonderform von Memory-Pools stellen ISAM-Pools dar. Diese Pools dienen zur Verarbeitung von ISAM-Dateien und werden nur in Verbindung mit NK-ISAM genutzt. Die folgenden Aussagen gelten also nicht für K-ISAM.

Es sind zwei Arten von ISAM-Pools zu unterscheiden:

Standard-Pools

Standard-Pools werden implizit vom Betriebssystem angelegt und genutzt, wenn der Benutzer eine ISAM-Datei eröffnet, die mit dem Kommando SET-FILE-LINK und dem Operanden BLOCK-CONTROL-INFO=WITHIN-DATA-BLOCK zugewiesen wurde und der Benutzer keinen eigenen ISAM-Pool zugewiesen hat. Der Geltungsbereich eines solchen Pool ist lokal. Soll darüber hinaus die Datei im SHARED-UPDATE-Modus verarbeitet werden (Operand SHARED-UPDATE=YES), ist der Geltungsbereich global.

Benutzer-Pools

Benutzer-Pools werden explizit durch den Benutzer angelegt und genutzt. Er bestimmt u.a. den Namen und den Geltungsbereich des Benutzer-Pool (lokal oder global). Bei globalen Benutzer-Pools ist ein weiterer Zugriffsschutz auf die Datei durch den Namen des Benutzer-Pool gegeben. Nur mit Kenntnis dieses Namens ist es einem Benutzer möglich, sich an den Benutzer-Pool anzuschließen. Da eine ISAM-Datei immer nur in einem Benutzer-Pool verarbeitet werden kann, kann über die gezielte Weitergabe des Namens der Kreis der Benutzer eingegrenzt werden. Weitere Dateischutzattribute wie z.B. Kennwörter werden überprüft, wenn der jeweilige Benutzer die Datei eröffnet. Folgendes Verfahren muß der Benutzer bei der Verwendung eines ISAM-Pool einhalten:

- Der Benutzer-Pool wird mit dem Kommando CREATE-ISAM-POOL angelegt und der Benutzer schließt sich an ihn an. Dabei wird der Name des Benutzer-Pool und sein Geltungsbereich festgelegt. Existiert ein globaler Benutzer-Pool schon, erfolgt lediglich der Anschluß an ihn.
- Über das Kommando ADD-ISAM-POOL-LINK legt der Benutzer einen Link-Namen für den Benutzer-Pool fest, unter dem der Benutzer-Pool im laufenden Auftrag angesprochen wird.
- Die Verarbeitung einer ISAM-Datei über den Benutzer-Pool wird mit dem Kommando SET-FILE-LINK gesteuert. Soll kein Standard-Pool verwendet werden, sondern der eingerichtete Benutzer-Pool, muß dieser über den Operanden POOL-LINK zugewiesen werden.
- Nach Beendigung der Dateiverarbeitung wird der Link-Name für den Benutzer-Pool mit dem Kommando REMOVE-ISAM-POOL-LINK aufgehoben.
- Über das Kommando DELETE-ISAM-POOL wird der Benutzer-Pool gelöscht bzw. der Benutzer vom Benutzer-Pool abgekoppelt.

Standard-Pools und Benutzer-Pools existieren vom Anlegen bis zum Löschen (bzw. bis zum letzten Abkoppeln bei globalen Pools). Vor Zuweisung des Speicherraums an andere Aufträge wird dieser durch das Betriebssystem gelöscht.

Eine ausführliche Beschreibung findet sich im Handbuch "BS2000 - DVS Einführung und Kommandoschnittstelle" [10].

6.8.12 User Serialization

Mit 'User Serialization' wird dem nicht-privilegierten Benutzer des BS2000 ein Mechanismus zur Verfügung gestellt, mit dem er in komfortabler Weise Serialisierungsprobleme hinsichtlich des Zugriffs mehrerer Prozesse oder Programmläufe auf gemeinsame Daten lösen kann. Der Mechanismus (semaphore-type mechanism) ermöglicht serielle Zugriffe auf vom Benutzer definierte Serialisierungskennungen.

Bei der Einrichtung einer Serialisierungskennung legt ein Benutzer u.a. ihren Namen und ihren Geltungsbereich fest. Der Name der Serialisierungskennung wird in einem zentralen Namenskatalog verwaltet, der nur dem Betriebssystem zugänglich ist.

Der Geltungsbereich legt fest, ob

- nur die laufende Task (Geltungsbereich LOCAL),
- alle Tasks der Benutzerkennung (Geltungsbereich GROUP),
- alle Tasks der Benutzergruppe (Geltungsbereich USER-GROUP) des OWNER, festgelegt auf dem Home-Pubset der laufenden BS2000-Sitzung, oder
- alle Tasks des Betriebssystems (Geltungsbereich GLOBAL)

die Serialisierungskennung benutzen dürfen. Damit wird sichergestellt, daß nur berechtigte Benutzer auf eine Serialisierungskennung zugreifen können.

Eine Serialisierungskennung muß einer Task entweder explizit oder implizit zugeordnet werden, bevor sie (exklusiv) belegt werden kann. Die Zuordnung kann ebenso explizit oder implizit wieder aufgehoben werden. Die Lebensdauer einer Serialisierungskennung endet, wenn ihr keine weitere Task mehr zugeordnet ist (siehe Handbuch "BS2000 - Makroaufrufe an den Ablaufteil" [16])

6.8.13 User Eventing

User Eventing ermöglicht dem nicht-privilegierten Benutzer des BS2000 die ereignisgesteuerte Synchronisierung von Abläufen in zwei oder mehreren Programmen in voneinander verschiedenen Tasks. Die Art des Synchronisationsereignisses wird zwischen den Partner-Prozessen mittels einer Ereigniskennung

Ereigniskennungen müssen vom Benutzer unter Angabe ihres Namens und ihres Geltungsbereichs explizit definiert werden. Der Name der Ereigniskennung wird in einem zentralen Namenskatalog verwaltet, der nur dem Betriebssystem zugänglich ist.

Der Geltungsbereich legt fest, ob

- nur die laufende Task (Geltungsbereich LOCAL),
- alle Tasks der Benutzerkennung (Geltungsbereich GROUP),
- alle Tasks der Benutzergruppe (Geltungsbereich USER-GROUP) des OWNER, festgelegt auf dem Home-Pubset der laufenden BS2000-Sitzung, oder
- alle Tasks des Betriebssystems (Geltungsbereich GLOBAL)

die Ereigniskennung benutzen dürfen. Damit wird sichergestellt, daß nur berechtigte Benutzer auf eine Ereigniskennung zugreifen können.

Für die Teilnahme an der Ereignissteuerung muß eine Task einer Ereigniskennung zugeordnet werden. Die Teilnahme an der Ereignissteuerung kann zu jedem beliebigen Zeitpunkt beendet werden. Die Ereigniskennung wird gelöscht, wenn ihr keine weitere Task mehr zugeordnet ist (siehe Handbuch "BS2000 - Makroaufrufe an den Ablaufteil" [16]).

6.9 Wiederverwendung von Objekten

Der Schutz von Information nach dem Löschen von Objekten wird dadurch gewährleistet, daß der freiwerdende Speicherplatz auch physikalisch gelöscht wird. Dies bedeutet, daß noch vorhandene Information mit binären Nullen überschrieben wird. Im BS2000 kann dabei zwischen folgenden Objekten unterschieden werden:

- Die Teile des Benutzeradreßraums, die einem Auftrag bei Auftragsbeginn vom Betriebssystem zugeordnet wurden und nicht im Memory-Pool liegen, werden bei Neuzuweisung automatisch physikalisch gelöscht.
- Der Inhalt von Systemausgabedateien wird beim Löschen mit dem Kommando DELETE-SYSTEM-FILE logisch gelöscht, d.h. der Last-Page-Pointer wird auf Null gesetzt. In die Dateien wird wieder ab Dateianfang geschrieben. Der Inhalt der Dateien, die den Systemausgabedateien mittels ASSIGN-Kommando zugewiesen wurden, wird ebenfalls logisch gelöscht. Die Katalogeinträge dieser Dateien bleiben bestehen, ihre Zuordnung zu den Systemdateien bleibt erhalten. Bei Auftragsende werden alle Systemdateien physikalisch gelöscht, die zugeordneten Dateien bleiben erhalten, sofern es sich nicht um temporäre Dateien handelt.
- Für Plattendateien des Benutzers gelten folgende Aussagen:

  Das Löschen einer Datei bedeutet im Normalfall das Austragen einer Datei aus dem zugehörigen Dateikatalog und die Rückgabe der belegten Speicherseiten an das Betriebssystem. Physikalisch gesehen existieren die Daten, die in der Datei hinterlegt waren, aber noch solange, bis sie durch neue überschrieben werden. Das physikalische Löschen der Daten kann auf mehrere Arten sichergestellt werden:

  - Durch eine Generierungsoption (Systemparameter DESTROY-OPTION) kann ein zwangsweises Löschen des Dateiinhalts beim Löschen einer Datei fest vorgegeben werden (siehe Sicherheitshandbuch für die Systemverwaltung).
  - Der Benutzer kann über folgende Kommandos und Operandenwerte gezielt das physikalische Löschen einer Datei veranlassen:

    CREATE-FILE ... ,DESTROY-BY-DELETE=YES
    MODIFY-FILE-ATTRIBUTES ... ,DESTROY-BY-DELETE=YES
    Bei einem späteren Löschen der Datei wird in jedem Fall der belegte Speicherplatz mit binär Null überschrieben, auch wenn im DELETE-FILE-Kommando keine weiteren Angaben gemacht werden.

    DELETE-FILE ... ,OPTION=DESTROY-ALL
    Der Datenbereich wird mit binär Null überschrieben, der Speicherplatz wird freigegeben und die Datei wird aus dem Dateikatalog gelöscht.

    Für Dateigenerationsgruppen und Dateigenerationen gilt
    CREATE-FILE-GROUP ... ,DESTROY-BY-DELETE=YES
    MODIFY-FILE-GROUP-ATTRIBUTES ... ,DESTROY-BY-DELETE=YES

Beim späteren Löschen der Dateigenerationsgruppe oder einer Dateigeneration wird in jedem Fall der belegte Speicherplatz mit binär Null überschrieben, auch wenn im DELETE-FILE-GROUP oder DELETE-FILE-GENERATION-Kommando keine weiteren Angaben gemacht werden. Dieses Attribut wird für die einzelnen Dateigenerationen zentral im Dateikatalog der zugehörigen Dateigenerationsgruppe hinterlegt.

DELETE-FILE-GROUP ... ,OPTION=DESTROY-ALL
Der Datenbereich wird mit binär Null überschrieben, der Speicherplatz wird freigegeben und die Dateigenerationsgruppe wird mit den dazugehörigen Dateigenerationen aus dem Dateikatalog gelöscht.

DELETE-FILE-GENERATION ... ,-
DELETE=GENERATIONS-BEFORE,OPTION=DESTROY-ALL

DELETE-FILE-GENERATION ... ,-
DELETE=GENERATIONS-AFTER,OPTION=DESTROY-ALL
Alle Dateigenerationen, deren Nummer kleiner/größer ist als die der Bezugsgeneration, werden aus dem Dateikatalog gelöscht, der Speicherplatz wird freigegeben und die Daten werden mit binär Null überschrieben. Wie bei der Erstellung von Dateigenerationen dürfen auch beim Löschen keine "Löcher" in der Folge der absoluten Generationsnummern entstehen.

– Banddateien können nicht direkt über BS2000-Kommandos gelöscht werden. Mit dem Kommando DELETE-FILE wird lediglich der Katalogeintrag einer Banddatei gelöscht, die Daten auf dem Magnetband bleiben jedoch erhalten.

  Der Benutzer kann veranlassen, daß bei der Verarbeitung von Banddateien weitere, auf dem Magnetband folgende Daten gelöscht werden. Dieses Verfahren kann dazu benutzt werden, Banddateien zu löschen. Voraussetzung dafür ist, daß Schreibzugriff auf das Magnetband möglich ist.

  – Löschen von Banddateien ab einer bestimmten Stelle.

    Dazu muß eine Banddatei auf eine der folgenden Arten katalogisiert bzw. zugewiesen worden sein:

```
create-file file-name=datei, ... ,destroy-by-delete=yes
modify-file-attributes file-name=datei, ... ,destroy-by-delete=yes
set-file-link...,file-name=datei,...,tape(...,
destroy-old-contents=yes)
```

    Wird die angegebene Banddatei ’datei’ als Ausgabedatei geschlossen, werden weitere auf dem Magnetband noch folgende (alte) Daten binär Null überschrieben. Ebenso werden bei einem Bandwechsel alle auf dem Magnetband bis zur Bandendemarke folgende (alte) Daten binär Null überschrieben.

– Löschen des gesamten Bandinhalts.

  Obiges Verfahren kann dazu benutzt werden, den gesamten Bandinhalt zu löschen. Es wird eine leere Banddatei an den Bandanfang geschrieben, die mit dem Kommando

```
create-file file-name=datei, ... ,destroy-by-delete=yes
```

  bzw.

```
set-file-link...,file-name=datei,...,tape(...,destroy-old-contents
=yes)
```

  katalogisiert bzw. zugewiesen wurde. Nach Schließen der Banddatei 'datei' werden alle folgenden Daten auf dem Magnetband binär Null überschrieben.

– Jobvariablen werden mit dem Kommando DELETE-JV gelöscht. Die beiden folgenden Fälle sind dabei zu unterscheiden:

  DELETE-JV ... ,OPTION=ALL

  Die Jobvariable wird aus dem Dateikatalog gelöscht, der dort belegte Speicherplatz wird freigegeben.

  DELETE-JV ... ,OPTION=DATA

  Der Wert der Jobvariablen wird logisch gelöscht, d.h. dem Wert der Jobvariablen, der im Katalogeintrag mitgeführt wird, wird die Länge Null zugewiesen. Der Katalogeintrag bleibt jedoch erhalten.

– Prozeßschalter werden automatisch bei Auftragsbeginn gelöscht, das heißt auf Null zurückgesetzt. Die Stellung von Benutzerschaltern bleibt über das Auftragsende hinaus erhalten. Sie müssen explizit durch den Benutzer mit dem Kommando MODIFY-USER-SWITCHES zurückgesetzt werden.

6.10 Organisatorische Maßnahmen des Benutzers zur Ergänzung des Zugriffsschutzes

Regeln zur Unterstützung des Zugriffsschutzes

Der vom Betriebssystem gebotene Zugriffsschutz sollte insbesondere im Hinblick auf sensitive Daten durch weitere organisatorische Maßnahmen von Seiten des Benutzers unterstützt werden. Generell sollten folgende Punkte beachtet werden:

- Die Zugriffserlaubnis zu Objekten des BS2000 sollte nur bei Notwendigkeit erteilt werden.
- Bei der Verwendung von Kennwörtern für den Zugriffsschutz sind die gleichen Maßnahmen zu berücksichtigen, wie für den Zugangsschutz (Seite 45).

Regeln zum Schutz von Prozedurdateien mit sensitiven Daten

Beim Starten von Stapelaufträgen müssen in der Auftragsbeschreibung, die in einer Prozedurdatei hinterlegt ist, alle zum Zugriff auf Dateien oder Benutzerkennungen relevanten Daten (Kennwort, Benutzerkennung, Abrechnungsnummer) zur Verfügung gestellt werden. Solche Prozedurdateien stellen ein erhöhtes Sicherheitsrisiko dar, da insbesondere benötigte Kennwörter hier im Klartext gespeichert sind, also nicht durch das Betriebssystem verschlüsselt werden. Die Prozedurdateien sollten daher durch die vorhandenen Zugriffsschutzmechanismen optimal geschützt werden. Darüber hinaus kann der Benutzer durch zusätzliche organisatorische Maßnahmen den Schutz dieser Dateien erhöhen, wie z.B.

- keine Ausdrucke von Stapelaufträgen erstellen, die sensitive Daten enthalten,
- sensitive Daten wie Kennwörter erst unmittelbar vor Auftragsbeginn und nur vorübergehend in diese Dateien schreiben
- keine Daten/Kommandos bei der Ausführung protokollieren (Operand LOGGING im Kommando BEGIN-PROCEDURE) oder
- Verwendung von SDF (ab Version 1.4).

Regeln zur Nutzung fremder Objekte

Die größte Gefahr durch die Nutzung fremder Objekte, insbesondere fremder Programme, geht von "Trojanischen Pferden" oder "Viren" aus.

Ein Trojanisches Pferd ist ein eigenständiges Programm, das vom Benutzer aktiv ins DV-System geladen wurde. Es bietet eine bestimmte Funktionalität (z.B. ein Spielprogramm), um so das Interesse des Benutzers zu wecken. Im Hintergrund werden die vom Programmierer dieses Programms gewünschten eigentlichen Funktionen ausgeführt, die dem Aufrufer des Programms jedoch verborgen bleiben. Sie können z.B. darin bestehen, Informationen zu sammeln, die den späteren Systemzugang ermöglichen. Insbesondere kann ein solches Programm ein Virus enthalten. Der Aufruf eines scheinbar harmlosen Programms kann somit gravierende Folgen haben.

Ein Virus ist ein Programmstück, welches, nachdem es in ein selbständig existierendes ’Wirts-Programm’ eingebracht wurde, die Fähigkeit besitzt, eine Kopie seiner selbst in ein weiteres, zuvor nicht infiziertes Programm einzubringen. Wird das ’Wirts-Programm’ ausgeführt, so werden die Anweisungen des Virus ebenfalls ausgeführt. Die Wirkung des Virus kann von der Ausgabe einer harmlosen Nachricht, über Datenverfälschung bis hin zur vollständigen Datenzerstörung reichen. Dabei muß die Wirkung nicht sofort eintreten. Sie kann zu einem späteren Zeitpunkt (z.B. einem fest vorgegebenen Datum) eintreten. In der Zwischenzeit hat das Virus Zeit, weitere Programme zu infizieren, so daß unbemerkt auch Archivbestände von dem Virus befallen sind, wenn die eigentliche Wirkung des Virus erst offensichtlich wird.

Aus der beschriebenen Funktionsweise lassen sich Maßnahmen ableiten, mit denen ein Benutzer sich gegen diese Bedrohungen schützen kann:

- Fremde Programme sollten nur aus vertrauenswürdigen Quellen bezogen werden. Es sollten niemals "Raubkopien" eingesetzt werden. Dadurch kann die Gefahr der Einpflanzung eines Ur-Virus vermindert werden.
- Fremde neue Programme sollten, soweit das möglich ist, auf separaten Anlagen auf ihre Virenfreiheit getestet werden. Erst wenn sichergestellt ist, daß sie nicht durch Viren, deren Wirkungsweise allgemein bekannt ist, infiziert sind, sollten sie in die Arbeitsumgebung eingebunden werden.
- Insbesondere ausführbare Dateien (Programme, Prozeduren) sollten mit Kennwörtern gegen Überschreiben geschützt werden. Solange ein Kennwort noch nicht in der Kennworttabelle eingetragen ist, kann ein Infizieren der so geschützten Programme durch den Aufruf bereits infizierter Programme ausgeschlossen werden.

7 Protokollierung des BS2000

Das BS2000 bietet drei Arten der Protokollierung, die für den Benutzer relevant sind:

- die Protokollierung des Auftragsablaufs,
- die Protokollierung von Daten zur Benutzer- und Betriebsabrechnung, die vom Benutzer für eigene Zwecke erweitert werden kann, und
- die Protokollierung sicherheitsrelevanter Ereignisse zu Revisionszwecken, die- unter bestimmten Voraussetzungenbenutzerspezifisch durchgeführt werden kann.

Die Protokollierung des Auftragsablaufs dient sowohl der eigenen Kontrolle des Benutzers hinsichtlich der von ihm ausgeführten Aktionen, um in Fehlersituationen Unterlagen für Analysezwecke zu erhalten, als auch der Nachweiskontrolle gegenüber dritten.

Für die Benutzerabrechnung werden task-spezifische Daten wie Verbrauch an CPU-Zeit, Anzahl der Ein-/Ausgaben, Belegung des Hauptspeichers etc. erfaßt. Diese Verbrauchsdaten ermöglichen es dem Betreiber des DV-Systems, den Benutzern die benötigten Betriebsmittel und Dienstleistungen in Rechnung zu stellen. Die für die Betriebsabrechnung erfaßten Daten geben eine zeitlich lückenlose Auskunft über die Auslastung und Verfügbarkeit des DV-Systems und können vom Betreiber zur Leistungs- und Engpaßanalyse verwendet werden. Der Benutzer hat die Möglichkeit, die Benutzer- und Betriebsabrechnung durch eigene Abrechnungssätze zu ergänzen.

Die Protokollierung sicherheitsrelevanter Ereignisse zu Revisionszwecken (Security Audit Trail, SAT) wird vom Sicherheitsbeauftragten festgelegt. Bei entsprechender Berechtigung, die durch die Benutzerverwaltung erteilt wird, kann der Benutzer die Protokollierung von Zugriffen auf Objekte, deren Eigentümer er ist, selbst steuern.

Im folgenden werden die drei für den Benutzer relevanten Arten der Protokollierung näher erläutert.

7.1 Protokollierung des Auftragsablaufs

Der Benutzer kann die Protokollierung des Auftragsablaufs mit dem Kommando MODIFY-JOB-OPTIONS festlegen. Dieses Kommando steuert:

- die Ausgabeform der Systemmeldungen (Operand INFORMATION-LEVEL),
- die Ausgabe von Bedienplatzmeldungen (Operand OPERATOR-INTERACTION),
- die maximale Anzahl an Ausgabesätzen in die Systemdateien SYSLST und SYSOPT (Operanden SYSLST-LIMIT, SYSOPT-LIMIT) und
- die Protokollierung des Auftragsablaufs für den laufenden Auftrag (Operand LOGGING).

Die Protokollierung von Prozedurabläufen wird mit dem Operanden LOGGING des Kommandos BEGIN-PROCEDURE festgelegt. Dieser Operand steuert:

- keine Protokollierung,
- Protokollierung der Kommandos bei Ausführung,
- Protokollierung der Daten bei Ausführung,
- Protokollierung der Kommandos und Daten bei Ausführung.

Protokollierung in die Systemdatei SYSOUT

Systemmeldungen und Bedienplatzmeldungen werden entsprechend den Vereinbarungen durch das Kommando MODIFY-JOB-OPTIONS standardmäßig in die Systemdatei SYSOUT geschrieben. Die Protokollierung von Prozedurabläufen, die mit dem Operanden LOGGING des Kommandos BEGIN-PROCEDURE festgelegt wurde, erfolgt ebenfalls in die Systemdatei SYSOUT.

Protokollierung in die Systemdatei SYSLST

Über den Operanden LOGGING=PARAMETERS(LISTING=YES) des Kommandos MODIFY-JOB-OPTIONS bzw. über den Operanden LOG=(LISTING=YES) des LOGON-Kommandos kann der Benutzer festlegen, daß das Ablaufprotokoll seines Auftrags zusätzlich in die Systemdatei SYSLST geschrieben wird. Soll die Protokollierung in SYSLST wieder aufgehoben oder unterbrochen werden, muß der Benutzer das Kommando MODIFY-JOB-OPTIONS LOGGING=PARAMETERS (LISTING=NO) eingeben.

Die Protokollierung gilt vom Zeitpunkt der Kommandoeingabe an und bezieht sich auf den laufenden Auftrag. Sie umfaßt folgende Aktionen:

- alle Eingaben des Benutzers mit Ausnahme von Kennwörtern (Kennwörter werden im Ablaufprotokoll durch eine Folge von 'S' ersetzt),
- alle Systemmeldungen, die auf dem Bildschirm ausgegeben werden,
- alle Meldungen von Programmen,
- Bedienplatzmeldungen und Operator-Meldungen (Operand OPERATOR-INTERACTION=YES).

Mit dem Kommando ASSIGN-SYSLST kann der Benutzer der Systemdatei SYSLST eine katalogisierte Datei als Ausgabeziel zuweisen. Protokolldaten bleiben dadurch über das Auftragsende hinaus erhalten.

Die Ausgabe des Ablaufprotokolls kann von der Systemverwaltung durch System Exits gesteuert werden. Werden keine System Exits eingesetzt, erzeugt das Betriebssystem nach dem Beenden eines Auftrags mit dem Kommando LOGOFF automatisch einen Ausdruck der Datei SYSLST. Die Ausgabe des Ablaufprotokolls kann explizit durch die Eingabe des Operanden NOSPOOL unterdrückt werden.

Bei der Protokollierung des Auftragsablaufs ist darüber hinaus zu beachten, daß Ausgaben, die standardmäßig auf SYSLST erfolgen, eine Maximalzahl von Sätzen nicht überschreiten dürfen. Diese Maximalzahl wird festgelegt:

- systemglobal für die jeweilige Jobklasse (siehe Handbuch "BS2000-Systemverwaltung" [17]) oder
- vom Benutzer im LOGON-Kommando (Operand PRINT) bzw. MODIFY-JOB-OPTIONS-Kommando (Operand SYSLST-LIMIT). Der angegebene Wert darf jedoch nicht größer sein als der systemglobale Wert.

Wird der Maximalwert überschritten, sind folgende zwei Fälle zu unterscheiden:

- Im Dialogbetrieb wird der Benutzer vom System gefragt, ob der Auftrag fortgesetzt oder abgebrochen werden soll. Bei Fortsetzung wird bis zur vorgegebenen Grenze wieder nach SYSLST protokolliert.
- Im Stapelbetrieb wird der Auftrag abgebrochen.

Anmerkung:

Der Maximalwert an Sätzen gilt nur für die standardmäßig in SYSLST protokollierten Systemmeldungen. Die bei der Ausgabe in SYSOUT zusätzlich in SYSLST protokollierten Meldungen werden bei der Überwachung des Maximalwerts nicht mitgezählt!

7.2 Protokollierung von Daten zur Benutzer- und Betriebsabrechnung

Das BS2000 protokolliert alle Daten, die zur Benutzer- und Betriebsabrechnung notwendig sind, in speziellen Abrechnungssätzen. Die Erfassung der Abrechnungsdaten wird auch als ACCOUNTING bezeichnet.

Die Steuerung der Datenerfassung für die Benutzer- und Betriebsabrechnung ist Aufgabe der Systemverwaltung (siehe Handbuch "BS2000- Systemverwaltung" [17]). Die Systemverwaltung legt insbesondere die Abrechnungsdatei fest, in die die verschiedenen Abrechnungssätze gespeichert werden. Die Auswertung der erfaßten Benutzer- und Betriebsabrechnungsdaten wird von speziellen Software- Produkten durchgeführt.

Dem Anwender im Teilnehmerbetrieb bietet das BS2000 die Möglichkeit, das ACCOUNTING durch das Erstellen von eigenen Abrechnungssätzen zu ergänzen. Für Anwenderprogramme stellt das Betriebssystem die ACCOUNTING-Schnittstellen AINF und AREC zur Verfügung:

- Mit dem Makro AINF kann sich ein Anwenderprogramm über den aktuellen Verbrauch an CPU-Zeit und Ein-/Ausgaben informieren.
- Der Makro AREC ist eine nicht-privilegierte Schnittstelle, über die eigene Abrechnungssätze des Benutzers erstellt und in die Abrechnungsdatei gespeichert werden können.

Mit dem Kommando WRITE-ACCOUNTING-RECORD kann der Benutzer ebenfalls eigene Abrechnungssätze erstellen und in die Abrechnungsdatei eintragen. Voraussetzung für das Schreiben benutzerspezifischer Abrechnungssätze ist eine entsprechende Berechtigung dazu. Diese wird von der Benutzerverwaltung mit dem Kommando ADD-USER oder MODIFY-USER-ATTRIBUTES über den Operanden MAX-ACCOUNT-RECORDS erteilt.

Folgende Abrechnungssätze können vom Benutzer erstellt werden:

- UDAT-Abrechnungssatz (Operand USER-DATA),
  Der UDAT-Abrechnungssatz enthält neben einer Benutzerkennzeichnung Grundinformation, z.B. Datum, Uhrzeit eines Aufrufs und variable Benutzerinformation (maximal 254 Byte).
- UACC-Abrechnungssatz (Operand USER-ACCOUNTING-STEP),
  Der UACC-Abrechnungssatz enthält neben einer Benutzerkennzeichnung den aktuellen Stand der Verbrauchswerte der wesentlichen Betriebsmittel.
- Frei definierbarer Abrechnungssatz.
  Ein frei definierbarer Abrechnungssatz enthält eine variable Benutzerinformation (maximal 492 Byte).

Frei definierbare Abrechnungssätze können nur mit dem Makro AREC oder von System-Exit-Routinen mit dem Makro $AREC erstellt werden. Dem Operanden MAX-ACCOUNT-RECORDS muß zuvor der Wert NO-LIMIT zugewiesen worden sein. Eine umfassende Beschreibung der Benutzer- und Betriebsabrechnung findet der Leser im Handbuch "BS2000-Systemverwaltung" [17] und in der technischen Beschreibung "BS2000-Auftragsverwaltungssystem" [18].

7.3 Protokollierung sicherheitsrelevanter Ereignisse

Das BS2000 verfügt über die Möglichkeit sicherheitsrelevante Ereignisse für bestimmte Objekte in speziellen Dateien aufzuzeichnen und für Revisionszwecke auszuwerten (Security Audit Trail, SAT [6]). Die Protokollierung sicherheitsrelevanter Ereignisse ist Aufgabe des Sicherheitsbeauftragten. Er bestimmt die Art und den Umfang der zu protokollierenden Ereignisse für eine Benutzerkennung und veranlaßt die Protokollierung. Die Auswertung der aufgezeichneten Daten erfolgt durch besonders autorisierte Personen (siehe Sicherheitshandbuch für die Systemverwaltung [13]).

Neben der Systemverwaltung hat auch der Eigentümer eines Objekts (in BS2000 V10.0: einer Datei) die Möglichkeit durch Setzen des Schutzattributs AUDIT (Seite 129 und Seite 135) die Protokollierung von Zugriffen auf dieses Objekt zu steuern. Voraussetzung dafür ist, daß ihm die entsprechende Berechtigung durch die Benutzerverwaltung erteilt wurde.

Auswahl

Welche Ereignisse als sicherheitsrelevant einzustufen und zu protokollieren sind, kann durch Auswahl festgelegt werden. Durch Auswahl kann im einzelnen bestimmt werden

- welche Benutzerkennungen,
- welche Ereignisarten und
- welche Objekte

für die Protokollierung berücksichtigt werden sollen.

Die Berechtigung zur Auswahl von Benutzerkennungen und Ereignisarten besitzt nur der Sicherheitsbeauftragte; die Auswahl der Objekte (in BS2000 V10.0: der Dateien) kann neben der Systemverwaltung auch der - dazu berechtigte - Eigentümer eines Objekts (einer Datei) vornehmen.

Die Ereignisarten, die für eine Datei protokolliert werden können, sind z.B. das Lesen oder Modifizieren von Daten, das Ändern von Sicherheitsattributen, das Umbenennen der Datei etc..

Alternative Auswahl-Logik

Der Sicherheitsbeauftragte kann zwei verschiedene Kombinationsregeln vorgeben, nach denen die durch Auswahl festgelegten Benutzerkennungen, Ereignisarten und Objekte zu verknüpfen sind (alternative Auswahl-Logik). Die beiden Kombinationsregeln bilden die Grundlage für die Entscheidung, ob ein Ereignis protokolliert werden soll oder nicht:

INDEPENDENT-Logik: (Benutzerkennung ODER Ereignisart ODER Objekt)

Diese Grundregel legt fest, daß ein Ereignis für die Protokollierung berücksichtigt wird, wenn entweder die Benutzerkennung oder die Ereignisart oder das Objekt durch Voraus-wahl festgelegt wurde.

FILES-BY-EVENTS-Variante: (Benutzerkennung ODER (Ereignisart UND Objekt))

Die alternative Kombinationsregel legt fest, daß ein Ereignis für die Protokollierung berücksichtigt wird, wenn entweder die Benutzerkennung oder die Ereignisart und das Objekt durch Auswahl festgelegt wurde. Diese Regel wird immer dann zur Anwendung kommen, wenn dem Benutzer Priorität eingeräumt werden soll, zu bestimmen, welche der Objekte (Dateien), deren Eigentümer er ist, sicherheitsrelevant sind. Die Anzahl der zu protokollierenden Ereignisse kann so möglichst klein gehalten werden.

7.3.1 SAT Alarm-Funktion

Die SAT-Alarm-Funktion erweitert den SAT-Funktionsumfang um ein wirksames Werkzeug, mit dem Verstöße gegen Sicherheitsmaßnahmen oder verdächtiges Verhalten im laufenden Betrieb sofort aufgespürt werden können.

Die Alarm-Funktion versetzt den Sicherheitsbeauftragten in die Lage, sofort verdächtiges Verhalten zu erkennen und nicht erst bei Auswertung der SAT-Protokolldateien, da an der Konsole der Systembedienung eine Meldung erscheint, die den Verstoß anzeigt. Dies ist besonders dann von Vorteil, wenn Sicherheitsverstöße augenscheinlich von Anwendern begangen werden. Der klassische Fall des Ausprobierens von Kennwörtern ist ein Beispiel für Sicherheitsverstöße von Anwendern.

Die Alarm-Funktion ersetzt nicht die SAT-Protokollierung und Auswertung der SAT-Protokolldateien, da auch die von der Alarm-Funktion erkannten Verstöße in den SAT-Protokolldateien eingetragen werden. Auch schwächt eine Vielzahl von Alarmen zu unterschiedlichen Ereignissen den Aufmerksamkeitswert des Alarms deutlich ab. Es sollte daher gut überlegt werden, welche Ereignisse einen Alarm auslösen.

Die SAT-Alarm-Funktion protokolliert, sofern SAT im Aufzeichnungsmodus ist,

- Ereignisse und Ergebnisse,
- Benutzerkennungen
- Information in Verbindung mit den Ereignissen
- Zeitraum innerhalb dem Ereignisse eintraten
- Anzahl der eingetretenen Ereignisse für einen Auftrag innerhalb eines definierten Zeitrahmens.

8 Resümee

Das BS2000 bietet mit den Software-Produkten ASECO [7] und SECOS [6] umfassenden Schutz vor unberechtigtem Zugriff auf Programme und Daten. Die Sicherheitsfunktionen des Betriebssystems ermöglichen im einzelnen:

- den Zugangsschutz durch Kennwort- und Chipkartenverfahren,
- die hierarchische oder projektbezogene Benutzerorganisation, Vergabe von Benutzerrechten und Benutzerverwaltung,
- den Zugriffsschutz durch Zugriffskontrollisten und weitere Schutzattribute sowie
- die Protokollierung sicherheitsrelevanter Ereignisse.

Das BS2000 stellt alle benötigten Funktionen für den sicheren Betrieb eines DV-Systems bereit. Der Einsatz des BS2000 im sicheren Betrieb ist jedoch an bestimmte Rahmenbedingungen geknüpft. Einerseits ergibt sich ein erhöhter Kontrollaufwand des Betriebssystems. Andererseits erhöht sich der Aufwand in der technischen und organisatorischen Handhabung, sowohl für den einzelnen Benutzer, z.B. durch die Vergabe von Schutzattributen, wie auch für den Betrieb des DV-Systems insgesamt, z.B. durch die Verteilung von Kompetenzen und der daraus resultierenden Verlängerung von Entscheidungswegen. Schließlich sind auch bestimmte Funktionseinschränkungen (siehe Anhang B) notwendige Voraussetzung für einen sicheren Betrieb.

Der Benutzer kann durch organisatorische Maßnahmen und Verhalten bedeutend zur Sicherheit eines DV-Systems beitragen. Voraussetzung hierfür ist, daß er sich seiner Verantwortung bewußt ist und das Angebot des BS2000 an Sicherheitsfunktionen korrekt und konsequent anwendet.

9 Anhang

9.1 Anhang A: Sicherheitsrelevante Kommandos des BS2000

1) Kommandos bezüglich der Schutzattribute für existierende Benutzerkennungen:

   MODIFY-LOGON-PROTECTION
   SET-LOGON-PROTECTION
   SHOW-LOGON-PROTECTION
   MODIFY-USER-PROTECTION

2) Kommandos bezüglich des Systemverwalterrechts USER-ADMINISTRATION:

   RESET-PRIVILEGE
   SET-PRIVILEGE
   SHOW-PRIVILEGE

3) Kommandos bezüglich der Verwaltung von Benutzergruppen:

   ADD-USER-GROUP
   MODIFY-USER-GROUP
   REMOVE-USER-GROUP
   SHOW-USER-GROUP

4) Kommandos zur Verwaltung von Benutzerkennungen:

   ADD-USER
   LOCK-USER
   MODIFY-USER
   SHOW-USER-ATTRIBUTES
   UNLOCK-USER

5) Kommandos zur Verwaltung von Objekten:

   ADD-FILE-ACL-ENTRY
   ADD-ISAM-POOL-LINK
   ADD-PASSWORD
   CREATE-FILE
   CREATE-FILE-ACL
   CREATE-FILE-GENERATION

CREATE-FILE-GROUP
CREATE-ISAM-POOL
CREATE-JV
DELETE-FILE
DELETE-FILE-ACL
DELETE-FILE-GENERATION
DELETE-FILE-GROUP
DELETE-ISAM-POOL
DELETE-JV
DELETE-SYSTEM-FILE
MODIFY-FILE-ACL-ENTRY
MODIFY-FILE-ATTRIBUTES
MODIFY-FILE-GENERATION-SUPPORT
MODIFY-FILE-GROUP-ATTRIBUTES
MODIFY-JOB-SWITCHES
MODIFY-JV
MODIFY-JV-ATTRIBUTES
MODIFY-JV-CONDITIONALLY
MODIFY-USER-SWITCHES
REMOVE-FILE-ACL-ENTRY
REMOVE-FILE-LINK
REMOVE-ISAM-POOL-LINK
REMOVE-PASSWORD
SECURE-FILE-ALLOCATION
SET-FILE-LINK
SHOW-FILE-ACL
SHOW-FILE-ATTRIBUTES

6) Kommandos zur Verwaltung von Guards:

a) Guards-Attribute
CREATE-GUARD
COPY-GUARD
MODIFY-GUARD-ATTRIBUTES
DELETE-GUARD
SHOW-GUARD-ATTRIBUTES

b) Zugriffsbedingungen
ADD-ACCESS-CONDITIONS
MODIFY-ACCESS-CONDITIONS
REMOVE-ACCESS-CONDITIONS
SHOW-ACCESS-ADMISSION
SHOW-ACCESS-CONDITIONS
SHOW-EVALUATED-CONDITIONS

Der GUARDS-Schutz wird den Objekten zugewiesen mit den Kommandos

für Dateien:

```
CREATE-FILE ...,PROTECTION=PARAMETERS(GUARD=PARAMETERS(READ=...,
                              WRITE=..., EXEC=...))

MODIFY-FILE-ATTRIBUTES ...,PROTECTION=PARAMETERS(GUARD=
                              PARAMETERS(READ=..., WRITE=..., EXEC=...))
```

für Bibliothekselemente mit den LMS-Anweisungen:

```
CREATE-ELEMENT ...,PROTECTION=PARAMETERS(GUARD=PARAMETERS(READ=...,
                                 WRITE=..., EXEC=...))

MODIFY-ELEMENT-PROTECTION ...,PROTECTION=PARAMETERS(GUARD=
                            PARAMETERS(READ=..., WRITE=..., EXEC=...))
```

für FITC-Ports

```
PROTECT-FITC-APPLICATION
```

9.2 Anhang B: Sicherheitsrelevante Generierungsoptionen

Um den unterschiedlichen Anforderungen der Betreiber hinsichtlich Performance und Sicherheit gerecht zu werden, kann das BS2000 entsprechend flexibel generiert werden. Der Benutzer hat die Möglichkeit die sicherheitsrelevanten Generierungsoptionen abzufragen (Kommando SHOW-SYSTEM-PARAMETERS oder Makro SINF) und kann sein Verhalten auf die eingestellten Werte abstimmen.

PASSWORD PENALTY

beeinflußt das Systemverhalten bei der Überprüfung von Kennwörtern:

`PWPENTI=0:` Default-Wert. Es wird keine Zeitstrafe vergeben.

`PWPENTI=1-60:` Nicht erfolgreiche Kennwort-Prüfungen werden mit einer Zeitstrafe belegt.

PASSWORD ENCRYPTION

steuert die Kennwort-Verschlüsselung:

`ENCRYPT=Y:` Kennwörter werden verschlüsselt im Benutzerkatalog und im Dateikatalog abgespeichert.

`ENCRYPT=N:` Default-Wert. Kennwörter werden unverschlüsselt im Benutzerkatalog und im Dateikatalog abgespeichert.

Größe der internen Kennworttabelle

begrenzt die Anzahl der Kennwörter in der internen Kennworttabelle eines Auftrags:

`PWACTIVE:` Wert 0 bis 15728639 (Default-Wert 15728639).

Anzahl der erlaubten Kennwörter je Prozeß

begrenzt die Anzahl von ADD-PASSWORD-Kommandos je Prozeß:

`PWENTERD:` Wert 0 bis 2147483647 (Default-Wert 2147483647).

Anzahl der erlaubten Fehlversuche bei der Kennworteingabe

begrenzt die Anzahl der Fehlversuche bei der Kennwort-Überprüfung je Task:

`PWERRORS:` Wert 0 bis 15728639 (Default-Wert 15728639).

FILE SHARING

steuert den Zugriff auf mehrbenutzbare Dateien:

`FSHARING=0:` Default-Wert. Nur Benutzerkennungen, die einen Eintrag im Benutzerkatalog des Pubset besitzen, können auf mehrbenutzbare Dateien des Pubset zugreifen.

`FSHARING=1:` Jede Benutzerkennung kann auf mehrbenutzbare Dateien eines Pubset zugreifen.

DESTROY-Option

beeinflußt das Systemverhalten beim Löschen von Datenbereichen:

`DESTLEV=0:` Default-Wert. Freigegebene Datenbereiche von Dateien werden nur dann mit binären Nullen überschrieben, wenn sie mit DESTROY-BY-DELETE=YES katalogisiert sind bzw. mit DESTROY-BY-DELETE=YES gelöscht werden.

`DESTLEV=1:` Alle Systemdateien zur Jobsteuerung (S.IN, SPOOL) werden mit DESTROY=YES eingerichtet.

`DESTLEV=4:` Freigegebene Datenbereiche aller Dateien werden mit binären Nullen überschrieben, unabhängig davon, ob sie mit DESTROY-ALL=YES katalogisiert sind bzw. mit DESTROY-ALL=YES gelöscht werden.

`DESTLEV=5:` Wie DESTLEV=4. Zusätzlich wird die F5-Label-Rekonstruktion mit einbezogen. Um sicherzustellen, daß auch nach einem irregulären Systemabbruch keine ungelöschten freien Bereiche vorhanden sind, werden alle freien PAM-Seiten auf binär Null gesetzt, die während der F5-Label-Rekonstruktion freigegeben werden.

`DESTLEV=6:` Wie DESTLEV=5. Zusätzlich werden die Extents, die einer Datei zugewiesen sind, beim logischen Erzeugen der Datei mit binären Nullen überschrieben, d.h. alle PAM-Seiten dieser Datei werden zum OPEN OUTPUT/OUTIN-Zeitpunkt auf binär Null gesetzt; falls die Datei mit PAM-Keys behaftet ist, werden diese ebenfalls auf binär Null gesetzt und mit einer ungültigen CFID versehen.

SVC79

beeinflußt das Systemverhalten beim Übergang von dem nicht-privilegierten Funktionsbereich TU in den privilegierten Funktionsbereich TPR. Der Übergang wird unter der Kontrolle der Generierungsoption nur für die Benutzerkennungen TSOS und SERVICE erlaubt:

`SVC79=0:` Default-Wert. Beim ersten SVC79 eines Programms wird eine Meldung an der Konsole des Operateurs ausgegeben.

`SVC79=1:` Beim ersten SVC79 eines Programms muß der Operateur den Übergang bestätigen.

`SVC79=2:` Der SVC79 ist nur für die Benutzerkennung SERVICE erlaubt. Beim ersten SVC79 eines Programms muß der Operateur den Übergang bestätigen.

`SVC79=3:` Der SVC79 ist nicht erlaubt.

Falls SVC79=3 generiert wurde, sind folgende Programme des BS2000-Grundausbaus nicht ablauffähig:

AUPMAIN,	PDPOOLS,
CMSTRACE,	PETRA,
COSMOS,	PPD,
IOTRACE,	SPCCNTRL,
MTTS,	TRSPOOL,
NKISTRAC,	TSOSMT.
PAMCONV,	

TEST LEVEL

begrenzt systemglobal den Read- und Write-Test-Level:

`RDTESTPR:` Wert 0 bis 9 (Default-Wert: 9)
`WRTESTPR:` Wert 0 bis 9 (Default-Wert: 9)

SECRET PAGES

beeinflußt das Systemverhalten bei der Ausgabe von Dumps:

`DUMPSEPA=1:` Die Ausgabe von Secret Pages wird nicht unterdrückt.

`DUMPSEPA=2:` Die Ausgabe von Secret Pages des Klasse-6-Speichers wird unterdrückt. Die Ausgabe von Secret Pages des Klasse-1-, Klasse-2-, Klasse-3-, Klasse-4- und Klasse-5-Speichers wird nicht unterdrückt.

`DUMPSEPA=3:` Die Ausgabe von Secret Pages des Klasse-1-, Klasse-2-, Klasse-3-, Klasse-4- und Klasse-5-Speichers wird unterdrückt. Die Ausgabe von Secret Pages des Klasse-6-Speichers wird nicht unterdrückt.

`DUMPSEPA=4:` Default-Wert. Die Ausgabe aller Secret Pages wird unterdrückt.

DUMPCL5P

steuert in CDUMP, ob der privilegierte Klasse-5-Speicher im User-Dump oder Area-Dump enthalten oder nicht enthalten sein soll:

`DUMPCL5P=0:` Default-Wert. Der gesamte Klasse-5-Speicher ist im User-Dump oder Area-Dump enthalten.

`DUMPCL5P=1:` Der privilegierte Klasse-5-Speicher wird bei der Ausgabe eines User-Dump oder Area-Dump unterdrückt.

CHECKPOINT/RESTART

beeinflußt das Systemverhalten bei der Ausgabe von Checkpoints und bei der Verarbeitung von Restarts:

`EREPASSW=N:` Default-Wert. Es wird kein Zufalls-Kennwort zur Sicherung der Checkpoint-Datei Manipulation generiert.

`EREPASSW=Y:` Zur Sicherung gegen Manipulation wird für jeden Checkpoint ein Zufalls-Kennwort generiert und in der Checkpoint-Datei gespeichert. Checkpoints können nur mit dem Makro WRCPT erstellt werden. CHKPT ist nur noch dann zulässig, wenn der zugehörige FCB zu einer *DUMMY-Datei gehört. Das Schreiben von Checkpoints am Bandende bei VLTFs (Very Large Tape Files) ist nicht möglich.

10 Fachwörter

Abrechnungsnummer (Account Number)

Bezeichnet ein Abrechnungskonto für die zugehörige Benutzerkennung. Eine Abrechnungsnummer kann mehreren Benutzerkennungen zugewiesen werden; eine Benutzerkennung kann über mehrere Abrechnungsnummern verfügen. Die Abrechnungsnummer wird bei der Zugriffskontrolle (LOGON-, ENTER-JOB-Kommando) ausgewertet.

Anschlußstelle

Stationsadresse einer Datensichtstation in einer BS2000- Konfiguration.

Authentisierung (Authentication)

Nachweis einer angegebenen Identität.
Synonym: Authentifizierung

Basic-ACL

siehe –→ Einfache Zugriffskontrolliste

Benutzer (User)

Er wird von einer Benutzerkennung repräsentiert. Der Begriff Benutzer ist ein Synonym für Personen, Anwendungen, Verfahren etc., die über eine Benutzerkennung Zugang zum Betriebssystem erhalten können.

Benutzerattribute

Merkmale einer Benutzerkennung, die von der Benutzerverwaltung vergeben und im Benutzerkatalog abgespeichert sind. Sie umfassen Benutzerrechte und Benutzerbeschreibungsdaten.

Benutzerattribute (User Attribute)

Alle Merkmale einer Benutzerkennung, die im Benutzerkatalog hinterlegt sind.

Benutzergruppe (User Group)

Zusammenfassung einer oder mehrerer Benutzerkennungen. Eine Benutzergruppe hat einen Namen (Benutzergruppenkennung) und besitzt eine Menge von Gruppenattributen (Gruppenpotential). Jede Benutzergruppe kann (muß aber nicht) einen eigenen Gruppenverwalter besitzen.

Benutzergruppeneintrag (Group Entry)

Sätze im Benutzerkatalog (ehemals $TSOS.TSOSJOIN, neuer Name siehe –→ Benutzerkatalog), die die Daten für eine Benutzergruppe enthalten.

Benutzergruppenkennung (Group Identificaton)

Name einer Benutzergruppe, der beim Einrichten der Benutzergruppe vergeben wird. Über die Benutzergruppenkennung wird die Benutzergruppe angesprochen.

Benutzerkennung (User Identification [USER-ID])

1) Maximal 8 Zeichen lange Datenstruktur
2) Eintrag im Benutzerkatalog. Anhand der Benutzerkennung erfolgt die Identifizierung beim Systemzugang. Die vom Betriebssystem verwalteten Dateien und Jobvariablen werden einer Benutzerkennung zugeordnet. Diese Zuordnung wird im Dateikatalog hinterlegt. Die Benutzerkennung stellt die Verbindung zwischen dem Benutzerkatalog und dem Dateikatalog dar.

Benutzerkatalog (Joinfile)

Datei, die die Benutzerattribute aller Benutzerkennungen eines Pubsets enthält. Ab V10.0 auf keybehaftet initialisierten Platten ist der Benutzerkatalog in zwei Dateien untergebracht: $TSOS.TSOSJOIN und $TSOS.SYSSRPM. Ab V10.0 auf keylos initialisierten Platten ist der Benutzerkatalog in der Datei $TSOS.SYSSRPM untergebracht.

Benutzerkommando (User Command)

Kommandos, die unter einer beliebigen Benutzerkennung im Systemmodus (/) oder auch im Programm-Modus mit CMD-Makros gegeben werden können.

Benutzerorganisation

Die Zusammenfassung von Benutzerkennungen zu Benutzergruppen. Hierdurch wird die Nachbildung bestehender Organisationsformen ebenso gestattet wie die projektorientierte Zusammenfassung von Benutzern.

Benutzerrechte

Alle an eine Benutzerkennung vergebenen und im Benutzerkatalog hinterlegten Benutzerattribute, die Rechte darstellen. Zu den Benutzerrechten zählt auch das Gruppenverwalterrecht.

Benutzerverwaltung (User Administration)

Alle Benutzerkennungen eines DV-Systems, die zur Verwaltung von Benutzerkennungen bzw. Benutzergruppen bezüglich Betriebsmitteln und Benutzerrechten berechtigt sind. Sie umfaßt die Gruppenverwalter sowie die systemglobale Benutzerverwaltung.
siehe –→ Systemglobale Benutzerverwaltung

Beweissicherung (Audit)

Grundfunktion eines sicheren Systems; Protokollierung von Abläufen und Aufbereitung der protokollierten Daten.

Dateikatalog (File Directory $TSOS.TSOSCAT)

Datei, die auf jedem Pubset vorhanden ist. Jede Datei und jede Jobvariable eines Pubsets sind im entsprechenden Dateikatalog eingetragen. Dateien von Privatplatten und Bändern können im Dateikatalog eingetragen sein. Ein Katalogeintrag enthält alle Attribute (Schutzattribute, Lage der verwalteten Daten usw.) einer Datei bzw. einer Jobvariablen (nicht aber die Zugriffskontrolliste ACL).

Datenschutz (Data Protection)

1. Im engeren Sinne gemäß Bundesdatenschutzgesetz die Aufgabe, durch den Schutz der personenbezogenen Daten vor Mißbrauch bei der Datenverarbeitung der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.

2. Im weiteren Sinne die Aufgabe, durch den Schutz der Daten vor Mißbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen. Datenschutz wird im Unternehmen realisiert durch

   – Einhaltung von Unternehmensgrundsätzen und Unternehmensrichtlinien,
   – Einhaltung von gesetzlichen Vorschriften,
   – problembewußtes Handeln,
   – zweckentsprechende Anwendung der Datensicherung.

Datensicherheit

Datensicherheit ist das Ergebnis der Datensicherung, also der technischen und organisatorischen Maßnahmen zum Schutz der Funktionsfähigkeit eines DV-Systems und der gespeicherten Information gegen Mißbrauch.

Datensicherung (Data Security)

Technisch-organisatorische Aufgabe, die Sicherheit von Datenbeständen und Datenverarbeitungsabläufen zu gewährleisten; d.h. insbesondere zu erreichen, daß

- der Zugriff zu Daten nur Berechtigten möglich ist,
- keine unerwünschte bzw. unberechtigte Verarbeitung von Daten erfolgt,
- die Daten bei der Verarbeitung nicht verfälscht werden,
- die Daten reproduzierbar sind. Diese Aufgabe wird gelöst durch
- in Hardware und Software enthaltene technische und organisatorische Vorkehrungen und Maßnahmen,
- übrige organisatorische sowie bauliche und personelle Vorkehrungen und Maßnahmen.

Datensichtstation (Terminal)

E/A-Gerät, bestehend aus Tastatur und Bildschirm, das über Netzsoftware dem Verarbeitungsrechner (VAR) angeschlossen ist. Die Datensichtstation kann dem VAR direkt (über MSN) angeschlossen sein oder sie kann eine Komponente eines Kommunikationsrechners sein (Adressierung über Stations- bzw. Transportsystemadresse).

Eigentümer (Owner)

Eigentümer eines Objekts ist eine Benutzerkennung, die Zugriffsrechte vergeben kann.

Einfache Zugriffskontrolliste (Basic Access Control List)

Einträge im Dateikatalog, die die Zugriffsrechte auf Dateien und Jobvariable für den Eigentümer, die Benutzergruppe und alle anderen Benutzerkennungen für Lesen, Schreiben und Ausführen regeln. (Nicht zu verwechseln mit der Zugriffskontrolliste ACL).

Erweiterte Sicherheitskontrolle (Advanced Security Control ASECO)

Mit der Verwendung von Chipkarten mögliche erweiterte Authentisierung des Benutzers und Nachvollziehbarkeit des Umgangs mit einem System.

FACS

File Access Control System - ermöglicht, Zugriffskontrollisten (ACL) für Dateien mit den Benutzerklassen USER, GROUP und OTHERS zu erstellen. Es gibt eine ACL pro Datei und jede ACL ist genau einer Datei zugewiesen. Der flexiblere Schutzmechanismus ist GUARDS.

First-Start

Beim First-Start werden Systemdateien neu eingerichtet. Vom System werden eine Reihe von Benutzerkennungen vergeben (TSOS, SYSPRIV, SYSDUMP, SERVICE, SYSGEN, SYSNAC, SYSHSMS, SYSUSER, SYSSNAP, SYSSPOOL, SYSAUDIT). Beim First-Start wird immer der Benutzerkatalog angelegt. Beim First-Start für einzelne Pubsets sind zwei Varianten möglich: Entweder Systemstart mit diesem Pubset oder IMCAT-Processing (logisches Hinzufügen eines weiteren Pubsets).

Frist

siehe –→ Schutzfrist

Funktionalitätsklasse (Functionality Class)

Klasse, die bestimmte Mindestanforderungen bezüglich der Funktionalität der Sicherheitsfunktionen an ein System der Informationstechnik stellt. Die Funktionalitätsklassen sind definiert innerhalb der "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)", 1. Fassung vom 11. Januar 1989, herausgegeben von der Zentralstelle für Sicherheit in der Informationstechnik im Auftrag der Bundesregierung.

Gemeinschaftlicher Datenspeicherbereich (Public Space)

Benannter Plattenspeicherbereich, der für eine definierte Anzahl von Benutzerkennungen des Betriebssystems verfügbar ist. Dieser Speicherbereich kann sich über einen oder mehrere Public Volume Sets (Pubsets) erstrecken.

Generierung (Generation)

1. Zusammenstellung von Software zu einem Betriebssystem.
2. Vorgang des Auswählens aus vom Hersteller gelieferter Software und des Überführens zu der beim Benutzer benötigten Form und Menge dieser Software sowie Festlegung der zu bedienenden Hardware.
3. Festlegen bestimmter Systemeinstellungen in Form von Systemparametern [z.B. Class-2-Options]. Festlegen des Kommando-Vorrats für den Operator und ähnliche betriebsvorbereitende Tätigkeiten

Gruppenkennung

siehe –→ Benutzergruppenkennung

Gruppenmitglied (Group Member)

Benutzerkennung, die einer Benutzergruppe zugeordnet ist. Der Gruppenverwalter kann einem Gruppenmitglied im Rahmen des Gruppenpotentials Betriebsmittel zuweisen.

Gruppenpotential

Enthält alle Betriebsmittel und Rechte, die an eine Benutzergruppe gebunden sind und an die Gruppenmitglieder der Benutzergruppe bzw. an hierarchisch untergeordnete Benutzergruppen vergeben werden können.

Gruppenverwalter (Group Administrator)

Ein Benutzer, der Gruppenpotentiale, Gruppenmitglieder und die untergeordnete Gruppenstruktur verwalten kann. Die Benutzerkennung, unter der diese Tätigkeiten ausgeführt werden dürfen, ist im Gruppenpotential der jeweiligen Benutzergruppe hinterlegt. Benutzerkennung, die mit dem Gruppenverwalterrecht ausgestattet ist.

Gruppenverwalterrecht (Group Administrator Privilege)

Berechtigt eine Benutzerkennung zur Verwaltung von- den Benutzerkennungen der eigenen Benutzergruppe und - hierarchisch untergeordneten Benutzerkennungen sowie - hierarchisch untergeordneten Benutzergruppen. Das Gruppenverwalterrecht kann in drei Ausprägungen vergeben werden, die den Umfang der erlaubten Tätigkeiten festlegen, diese sind:

- Manage Resources
- Manage Members
- Manage Groups.

Guard

Objekt der Bedingungsverwaltung GUARDS. In einem Guard werden Bedingungen gesammelt, die von der Standard-Bedingungsverwaltung von GUARDS auf Anfrage ausgewertet werden.

GUARDS

(generally usabel access control administration system) Objektverwaltung für Guards.

Identifizierung (Identification)

Verfahren zur Erkennung eines Sachverhalts, einer Person oder eines Objekts.

Installation

1. Vorgang des Bereitstellens von Gerätetechnik und Software
2. Bei einem Benutzer vorhandene Gerätetechnik und Software.

IT-Sicherheitskriterien

Kriterien zur Bewertung der Sicherheit von Systemen der Informationstechnik (IT).
siehe –→ Sicherheitskriterien

Katalogkennung (Catalog Identification CATID)

Kennzeichnet einen Pubset durch ein oder [ab V10.0] mehrere Zeichen. 1. Viertes Zeichen der Volume Serial Number. Dieses Zeichen ist bei allen
Platten eines Pubsets gleich.
2. Bis zu vier Stellen bei V10.0 <cat-id 1...4>

Kennwort (Password)

Folge von Zeichen, die der Benutzer eingeben muß, um den Zugriff zu einer Benutzerkennung, einer Datei, einer Jobvariablen, einem Netzknoten oder einer Anwendung zu erhalten. Das Benutzerkennungs-Kennwort dient zur Authentifizierung des Benutzers. Es dient dem Zugangsschutz. Das Datei-Kennwort dient zur Überprüfung der Zugriffsberechtigung beim Zugriff auf eine Datei (Jobvariable). Es dient dem Zugriffsschutz. Synonym: Paßwort

Kommandooberfläche

Stellt die Schnittstelle zwischen Mensch und Betriebssystem dar. Dem Benutzer werden über Kommandos Leistungen des Betriebssystems zur Verfügung gestellt. Die Leistungen der Kommandooberfläche sind auch über die Programmieroberfläche erreichbar.

Kommandoprofil (Command Profile)

siehe –→ Profile

Objekt (Object)

Passives Element eines DV-Systems, das Informationen enthält oder aufnimmt und auf das eine Operation wie Lesen, Schreiben, Ausführen etc. angewendet werden kann. Der Zugriff auf ein Objekt impliziert im allgemeinen den Zugriff auf Daten, die das Objekt enthält.

offline-Betrieb

1. Arbeitsweise einer funktionellen Einheit, wenn sie nicht unter der direkten Steuerung eines Rechners steht.
2. Weder gesteuert noch verbunden mit einem Rechner (Gegensatz zu online-Betrieb).

online-Betrieb

1. Arbeitsweise einer funktionellen Einheit, wenn sie unter der direkten Steuerung eines Rechners steht.
2. Fähigkeit eines Benutzers zur interaktiven Arbeit mit einem Rechner.
3. Benutzerzugriff zu einem Rechner über eine Datensichtstation.
4. Gesteuert von oder verbunden mit einem Rechner (Gegensatz zu offline-Betrieb)

Operator-Role

Zusammenfassung einer Menge von Routing-Codes unter einem Namen. Es sind beliebige Kombinationen von 40 Routing-Codes möglich.

Personenbezogene Beweissicherung (Personal Audit for Individual Accountibility)

Nachvollziehbarkeit des Umgangs mit einem System. Identifikation entweder in Form: eine Benutzerkennung entspricht einem Benutzer oder ein Benutzer verfügt über eine Chipkarte oder ein Benutzer darf ausschließlich eine Bedienstation benutzen.

Privilegienverwalter

Dieser Begriff sollte nicht verwendet werden. Im Zusammenahng mit der Sicherheit spricht man vom Sicherheitsbeauftragten.

Profil (Profile)

Ein einer Benutzerkennung zugeordneter Kommando-Vorrat, dessen Zulässigkeit über Syntax-Dateien sichergestellt wird.

Programmieroberfläche

Schnittstelle zwischen Programmen bzw. zwischen Programmen und Betriebssystem. Die Leistungen werden über Programmiersprachen zur Verfügung gestellt.

Public Volume Set (Pubset)

Durch eine Katalogkennung (Catid) definierte Menge von gemeinschaftlichen Plattenspeicher-Einheiten.

Qualitätsstufe (Assurance Level)

Hierarchische Unterteilung bezüglich der Qualität eines Systems der Informationstechnik (IT-Systems). Bei der Evaluation wird die Qualität eines IT-Systems bewertet. Anhand dieser Bewertung erfolgt eine Einstufung in eine der Qualitätsstufen Q0 bis Q7.

Rolle (Role)

Gruppierung von Attributen, die einem Subjekt zugeordnet werden können, z.B. Sicherheitsbeauftragter.

Sammelprivileg

Zusammenfassung systemglobaler Privilegien zu einer Gruppe, die mit einem selbstgewählten Namen bezeichnet wird.

Schutzattribute (Security Attributes)

Sicherheitsrelevante Eigenschaften eines Objekts, die Art und potentielle Möglichkeit des Zugriffs auf dieses Objekt festlegen. Für Dateien gibt es folgende Schutzattribute: ACCESS/USER-ACCESS, SERVICE-bit, AUDIT-Attribut (NONE/SUCCESS/FAILURE/ ALL), RDPASS, WRPASS,EXPASS, RETPD, Basic-ACL, ACL und GUARD.

Schutzfrist (Retention Period)

Zeitintervall in Tagen, in dem ein Objekt (z.B. Datei) nicht verändert oder gelöscht werden kann.

SHUTDOWN

Vorgang der geordneten Systembeendigung (einschließlich des Sicherns spezieller Systemdateien).

Sichere Generierung

Generierung des BS2000, die alle sicherheitsrelevanten Einstellungen zur Gewährung der Sicherheit aktiv benutzt.

Sichere Hardware-Konfiguration

Installierte Gerätetechnik (einschließlich Datenfernübertragungstechnik und Netz), die keinen Sicherheitseinschränkungen unterliegt.

Sicheres BS2000

BS2000, das in einer sicheren Generierung erzeugt wurde. Synonyme Begriffe dazu sind: 'F2/Q3-System' oder 'evaluiertes System'. Das Gegenteil eines 'sicheren BS2000' ist nicht ein 'unsicheres BS2000', sondern ein System, das beispielsweise nicht-bewertete Teile enthält oder das nicht den Kriterien F2/Q3 entspricht bzw. ein System, das nicht gemäß der empfohlenen Konfiguration betrieben wird.

Sicherheitsbeauftragter (Security Administrator, Security Officer)

1. Sicherheitsbeauftragter im herkömmlichen Sinne:
   Organisatorisch-administrative Institution.
2. Die Kennung des Sicherheitsbeauftragten kann mit Hilfe des STARTUP-PARAMETER-SERVICE festgelegt werden. Bei Auslieferung ist die Kennung des Sicherheitsbeauftragten SYSPRIV. Der Sicherheitsbeauftragte hat das Recht, systemglobale Privilegien an Benutzerkennungen zu vergeben und zu entziehen. Er hat das Recht, die SAT-Protokollierung aus- und einzuschalten, Operator-Roles zu verwalten sowie Benutzerkennungen und Ereignisse für die Protokollierung auszuwählen.

Sicherheitskriterien (Security Criteria)

Dienen der Bewertung der Sicherheit von Systemen der Informationstechnik. Sie bestehen aus Funktionalitätsklassen und Qualitätsstufen. Dies wird in Form von Fx/Qy (Funktionalitätsklasse x und Qualitätsstufe y) dargestellt; Beispiel: F2/Q3 bedeutet Funktionalitätsklasse 2 und Qualitätsstufe 3.

Sicherheitsverwalter

siehe –→ Sicherheitsbeauftragter

Standardzugriffskontrolle (Standard Access Control)

Besteht aus den in den Kommandos

```
create-file... oder
modify-file-attributes...
```

festgelegten Zugriffsrechten ACCESS und USER-ACCESS.

Subjekt (Subject)

Aktives Element eines DV-Systems, von dem eine Operation wie Lesen, Schreiben, Ausführen u.ä. ausgehen kann, die einen Informationsfluß bewirkt oder den Systemzustand ändert, z.B. Kennung, Programm, Programmteil.

System-Privileg USER-ADMINISTRATION

Berechtigt eine Benutzerkennung alle Benutzerkennungen und alle Benutzergruppen eines DV-Systems zu verwalten.

Systemeinleitung (STARTUP)

Laden der Betriebssystem-Software. Es wird unterschieden in:

- DIALOG-STARTUP
- FAST-STARTUP
- QUICK-STARTUP
- AUTOMATIC-STARTUP

Die Varianten der Systemeinleitung unterscheiden sich durch unterschiedlichen Automatisierungsgrad und unterschiedlichen Rückbezug auf die letzte Systemeinleitung.

Systemglobale Benutzerverwaltung (User Administration)

Sie umfaßt die Verwaltung von Benutzerkennungen und Benutzergruppen bezüglich Betriebsmitteln und Benutzerrechten, das Neueinrichten, Modifizieren und Löschen von Benutzerkennungen und Benutzergruppen.

Systemglobale Privilegien

Alle mit dem Kommando /SET-PRIVILEGE vergebbaren Privilegien sowie das Privileg des Sicherheitsbeauftragten und das Privileg der Kennung TSOS. Diese sind im einzelnen im Abschnitt "Privilegien der Systemverwaltung" aufgezählt. ’Systemglobale Privilegien’ und ’Systemverwalterrechte’ sind identisch.

Systemlauf (Session)

Vorgänge/Aktivitäten zwischen Systemeinleitung und Systembeendigung.

Systemressourcen (System Resource)

Ein Betriebsmittel eines Rechnersystems, das von einem Job oder einer Task angefordert bzw. freigegeben werden kann.

Systemverwalterrechte

Rechte, die für die Steuerung und Überwachung des laufenden BS2000-Betriebs vorgesehen sind. Im einzelnen sind dies

- alle mit dem Kommando SET-PRIVILEGE vergebbaren Rechte,die Rechte des Sicherheitsbeauftragten sowie
- die Rechte, die an die Benutzerkennung TSOS geknüpft sind.

Synonym: Systemglobale Rechte

Systemverwaltung (System Administration)

1. Struktureinheit im Rechenzentrum
2. Personenkreis, der Benutzerkennungen verwendet, an die systemglobale Rechte gebunden sind.

Zugangsklasse (Access Class)

Es werden in SECOS folgende Zugangsklassen unterschieden:

- DIALOG-ACCESS oder DIALOG (Zugang vom Teilnehmersystem)
- BATCH-ACCESS oder BATCH (Zugang für Stapelaufträge vom gleichen Rechner)
- RBATCH-ACCESS oder RBATCH (Zugang von Fernstapelstationen)

Zugangsschutz

Beinhaltet alle Methoden zum Schutz eines DV-Systems vor unberechtigtem Systemzugang.

Zugriffsberechtigter (Authorized User)

Subjekt, das auf ein Objekt zugreifen darf, z.B. Benutzerkennung auf Datei

Zugriffsberechtigung (Access Admission)

Legt fest, welches Subjekt auf welche Weise auf ein Objekt zugreifen darf.

Zugriffskontrolliste (Access Control List [ACL])

Systemdatei, die die Zugriffsrechte auf gemeinschaftliche Plattendateien eines Public Volume Set enthält. Sie ermöglicht die Verfeinerung des Zugriffsschutzes bis auf die Ebene eines Benutzers.

Zugriffsrecht (Access Right)

Recht eines Subjekts, auf ein Objekt mit einem vorgegebenen Zugriffsrecht zugreifen zu dürfen. Zugriffsrechte regeln das Lesen, Schreiben und Ausführen.

Zugriffsschutz

Zugriffsschutz bezeichnet die Regeln, nach denen in einem DV-System Subjekte auf Objekte zugreifen können und die Methoden, mit denen die Einhaltung dieser Regeln sichergestellt werden kann.

Zugriffstyp (Access Type)

Allgemein: Legt fest, wie auf ein Objekt zugegriffen werden kann. Die Zugriffstypen für Dateien sind Lesen, Schreiben und Ausführen. Die Zugriffstypen für Jobvariablen sind Lesen und Schreiben. Der Zugriffstyp für Memory Pools ist das Anschließen an den Memory Pool (ENAMP). Der Zugriffstyp für die Serialization ist das Anschließen an die Serialisierungskennung (ENASI). Der Zugriffstyp für die Ereignissteuerung ist das Anschließen an die ereignisgesteuerte Verarbeitung (ENAEI). Synonym: Zugriffsart

Literatur

[1] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz, BDSG) in Bundesgesetzblatt Teil I, Z 1997 A, 1977, Nr. 7, ausgegeben zu Bonn am 1.2.1977 *

[2] Landesdatenschutzgesetze der einzelnen Länder *

[3] **IT-Sicherheitskriterien:**
Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT) /hrsg. von d. ZSI, Zentralstelle für Sicherheit in d. Informationstechnik im Auftrag. d. Bundesregierung - 1. Fassung vom 11. Januar 1989. - Köln: Bundesanzeiger, 1989
ISBN 3-88784-192-1
NE: Zentralstelle für Sicherheit in der Informationstechnik <Bonn> *

[4] **RFA V11.0**
(BS2000/OSD)
Remote File Access
Benutzerhandbuch

Zielgruppe
BS2000/OSD-Anwender
Inhalt
Das Handbuch erläutert die Grundlagen des RFA-Konzepts. Alle RFA-Kommandos sind ausführlich beschrieben, wie auch die Besonderheiten von DVS-Kommandos beim Zugriff auf Dateien in einem fernen System mit RFA.

[5] Katastrophen in Rechenzentren
Leitfaden für Katastrophenpläne
Herausgeber: Siemens AG, Bereich Datentechnik
Bestell-Nr. U1700-J-Z18-1
Ausgabe April 1984

[6] **SECOS V2.0A**
(BS2000/OSD)
Security Control System
Benutzerhandbuch

Zielgruppe
- BS2000-Systemverwalter
- BS2000-Anwender, die den erweiterten Zugriffsschutz für Dateien nutzen

Inhalt
Leistung und Anwendung der vier Funktionseinheiten:
- SRPM (Privilegien und Betriebsmittel verwalten)
- FACS (erweiterter Zugriffsschutz für Dateien)
- GUARDS (Zugriffsbedingungsverwaltung und -auswertung für Objekte)
- SAT (Protokollierung und Auswertung sicherheitsrelevanter Daten, Ereignisüberwachung mit Alarmfunktion).

[7] **ASECO** (BS2000)
Advanced Security Control
Benutzerhandbuch

Zielgruppe
BS2000-Systemverwaltungen, die den Zugangsschutz mit Chipkarten realisieren.

Inhalt
- Hard-/Softwarekonfiguration
- Verfahren der Authentisierung
- Einsatz des Chipkartenschutzes im Teilnehmer- und im Transaktionsbetrieb
- Hinweise zur Installation von ASECO

Einsatz
Zugangsschutz mit Chipkarten

[8] **MAREN** (BS2000)
für den Administrator Systemverwalterhandbuch

Zielgruppe
RZ- und Systemverwalter

Inhalt
Beschreibung des Magnetdatenträger-Archivierungssystems im Rechnernetz (MAREN-System) zur Verwaltung von Datenträgerbeständen in einem BS2000-Rechenzentrum.

[9] BS2000
Benutzerkommandos (ISP-Format)
Benutzerhandbuch

Zielgruppe
BS2000-Anwender (nicht privilegiert)
Inhalt
Alle BS2000-Systemkommandos in lexikalischer Reihenfolge mit Hinweisen und Beispielen.
Folgende Liefereinheiten sind berücksichtigt:
BS2000-GA, MSCF, JV, FT, TIAM
Einsatz
BS2000-Dialogbetrieb, -Prozeduren, -Stapelbetrieb

[10] **BS2000/OSD-BC V1.0**
Benutzer-Kommandos (SDF-Format)
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an den nichtprivilegierten BS2000/OSD-Anwender (Privileg STD-PROCESSING).
Inhalt
Es enthält alle BS2000/OSD-Kommandos, die dem nichtprivilegierten Anwender im Grundausbau des BS2000/OSD zur Verfügung stehen. Der Anwender erhält Hinweise zur Kommandoeingabe im Dialog- und Stapelbetrieb. Der Anhang enthält u.a. Hinweise zu SDF-P. Beschrieben ist BS2000/OSD-BC V1.0. Zusätzlich wurde u.a berücksichtigt:
- SDF V3.0A
- SDF-P BASYS V1.0B
- SPOOL V2.7A
- RSO V2.2A
- JV V11.0A
- RFA V11.0A
- FT V5.0A

[11] **BS2000/OSD-BC V1.0**
DVS Einführung und Kommandoschnittstelle
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an alle BS2000/OSD-Anwender.
Inhalt
Das Benutzerhandbuch beschreibt die Kommandoschnittstelle des DVS im Funktionsumfang der Version BS2000/OSD-BC V1.0. Nach einem einführenden Teil und zugriffsmethodenspezifischen Abschnitten werden die Kommandos des DVS (SDF-Format) dargestellt.

[12] **BS2000/OSD-BC V1.0**
DVS Assembler-Schnittstelle
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an alle BS2000/OSD-Assembler-Programmierer.
Inhalt
Es beschreibt die Makroschnittstelle des DVS im Funktionsumfang der Version BS2000/OSD-BC V1.0. Nach einem einführenden Teil und zugriffsmethodenspezifischen Abschnitten werden in lexikalischer Form die Makros dargestellt.

[13] **BS2000/OSD-BC V1.0**
Sicherheitshandbuch für die Systemverwaltung

Zielgruppe
Das Handbuch wendet sich an die Systemverwaltung des Betriebssystems BS2000/OSD.
Inhalt
Beschrieben werden sicherheitsrelevante Funktionen und Aspekte in den Bereichen Installation und Generierung, Benutzerverwaltung, Systemverwaltung, Systembedienung, Diagnose und Datenfernverarbeitung.

[14] BS2000
Systemübersicht
Technische Beschreibung

Zielgruppe
- BS2000-Anwender und -Betreiber, die sich für den technischen Hintergrund ihres Systems interessieren (Softwareentwickler, Systemanalytiker, RZ-Leiter, Systemverwalter)
- Informatiker, die ein konkretes "General-Purpose"-Betriebssystem studieren wollen

Inhalt
- Charakteristika des BS2000 (Einsatz- und Leistungsmerkmale, Oberfläche, Betriebsmittel, interner Aufbau und Abläufe)
- mögliche Hardwarekonfigurationen
- Teilsysteme des BS2000 (Basissystem, Datenverwaltungssystem, Auftragsverwaltungssystem, Programmiersystem, Datenkommunikationssystem, Transaktionsmonitor, Systemadministration, Bediensystem)

Bestellnummer
U3210-J-Z53-1

[15] **JV V11.0A**
(BS2000/OSD)
Jobvariablen
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich sowohl an den nichtprivilegierten als auch privilegierten BS2000/OSD-Anwender.
Inhalt
Es beschreibt die Anwendung des Software-Produkts JV (Jobvariablen). Es enthält die Beschreibungen der Kommandos und Makros zur Verwaltung der JVs und zur bedingungsabhängigen Auftragssteuerung.

[16] **BS2000/OSD-BC V1.0**
Makroaufrufe an den Ablaufteil
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an alle BS2000/OSD-Assembler-Programmierer.
Inhalt
Das Handbuch enthält eine Zusammenstellung der Makroaufrufe an den Ablaufteil, die ausführliche Beschreibung jedes Makroaufrufs mit Hinweisen und Beispielen, einschließlich der Jobvariablen-Makros, sowie einen ausführlichen allgemeinen Lernteil.

[17] **BS2000/OSD-BC V1.0**
Systemverwaltung
Benutzerhandbuch

Zielgruppe
BS2000/OSD-Systemverwalter
Inhalt
Das Handbuch beschreibt die Maßnahmen, die die Systemverwaltung treffen muß, um das Betriebssystem zu verwalten, sowie die notwendigen Kommandos. Die Neuausgabe enthält einige neue Funktionen und Aufgabenbereiche, insbesondere für die Verwaltung und Steuerung der Caching-Medien im BS2000/OSD. Das Handbuch enthält folgende Kapitel:
– Systemadministration
– Systemsteuerung und -optimierung
– Datensicherheit
– Datensicherung
– Automatisierung der Systembedienung
– Kommandos

[18] BS2000
Auftragsverwaltungssystem
Technische Beschreibung

Zielgruppe
- BS2000-Anwender und -Betreiber, die sich für den technischen Hintergrund ihres Systems interessieren (Softwareentwickler, Systemanalytiker, RZ-Leiter, Systemverwalter)
- Informatiker, die ein konkretes "General-Purpose"-Betriebssystem studieren wollen

Inhalt
Funktionen und Realisierungsprinzipien
- des Job-Management-Systems
- des Mehrrechnersystems
- des Job-Variable-Systems
- des SPOOL
- des Abrechnungssystems

Bestellnummer
U3213-J-Z53-1

[19] **PERCON V2.5A**
(BS2000/OSD)
SDF-Format
Benutzerhandbuch

Zielgruppe
BS2000/OSD-Anwender
Inhalt
Das Handbuch beschreibt die Vorgehensweise und die Anweisungen, wie Daten auf beliebige Datenträger übertragen und umgesetzt werden können. Häufige Anwendungsfälle werden durch Beispiele erklärt.

[20] **SPOOL V2.7A**
(BS2000/OSD)
Teil 1, System
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an BS2000/OSD-Anwender, Systemverwalter und RSO-Geräteverwalter.
Inhalt
Es werden der Betrieb von SPOOL V2.7A mit den verfügbaren Kommandos, Makros, System-Exits und Systemmeldungen, außerdem die Arbeit mit Druckern und Datenträgern beschrieben. Die Ergänzungen von SPOOLAPA V1.0A und RSO V2.2A wurden berücksichtigt.

[21] * Information Technology Security Evaluation Criteria, Version 1.2 vom Juni 1991, ISBN 92-826-3004-8

Mit * markierte Titel sind nicht von der Siemens Nixdorf Informationssysteme AG oder der Siemens AG herausgegeben.

Bestellen von Handbüchern

Die aufgeführten Handbücher finden Sie mit ihren Bestellnummern im *Druckschriftenverzeichnis* der Siemens Nixdorf Informationssysteme AG. Neu erschienene Titel finden Sie in den *Druckschriften-Neuerscheinungen*.

Beide Veröffentlichungen erhalten Sie regelmäßig, wenn Sie in den entsprechenden Verteiler aufgenommen sind. Wenden Sie sich bitte hierfür an Ihre zuständige Geschäftsstelle. Dort können Sie auch die Handbücher bestellen.

Stichwörter

B

C

M

S

V

Inhalt

BS2000/OSD-BC V1.0

Sicherheitshandbuch für den Benutzer

Zielgruppe

Anwender im Teilnehmerbetrieb des BS2000/OSD-BC V1.0

Inhalt

– Vorstellung der Sicherheitsfunktionen des BS2000/OSD-Betriebssystems
– Einsatzhinweise und Empfehlungen, wie Daten und Programme vor unberechtigtem Zugriff geschützt werden können.

Ausgabe: **April 1993**

Datei: **SICHBEN.PDF**