



SAP AG
Neurottstr. 16
D-69190 Walldorf

R/3 Security

R/3 Security Guide: VOLUME I

An Overview of R/3 Security Services

Version 2.0a : English

March 22, 1999

Copyright

©Copyright 1999 SAP AG. All rights reserved.

No part of this documentation may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG.

SAP AG further does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP AG shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials. The information in this documentation is subject to change without notice and does not represent a commitment on the part of SAP AG in the future.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT® and EXCEL® and SQL-Server® are registered trademarks of Microsoft Corporation.

IBM®, OS/2®, DB2/6000®, AIX®, OS/400® and AS/400® are a registered trademark of IBM Corporation.

OSF/Motif® is a registered trademark of Open Software Foundation.

ORACLE® is a registered trademark of ORACLE Corporation, California, USA.

INFORMIX®-OnLine *for SAP* is a registered trademark of Informix Software Incorporated.

UNIX® and X/Open® are registered trademarks of SCO Santa Cruz Operation.

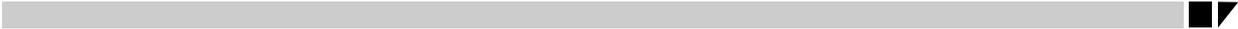
ADABAS® is a registered trademark of Software AG.

SECUDE® is a registered trademark of GMD-German National Research Center for Information Technology.

SAP®, R/2®, R/3®, RIVA®, ABAP®, SAPoffice®, SAPmail®, SAPaccess®, SAP-EDI®, SAP ArchiveLink®, SAP EarlyWatch®, SAP Business Workflow®, R/3 Retail® are registered trademarks of SAP AG.

SAP AG assumes no responsibility for errors or omissions in these materials.

All rights reserved.



Copyright

Table of Contents

CHAPTER 1: INTRODUCTION	1-1
CHAPTER 2: SECURITY ASPECTS.....	2-1
Authentication	2-1
Authorization	2-2
Integrity	2-2
Privacy	2-3
Obligation (non-repudiation)	2-3
Auditing and Logging	2-3
CHAPTER 3: THE R/3 SECURITY SERVICES.....	3-1
User Authentication.....	3-2
R/3 Password Rules	3-2
Single Sign-On / Smart Card Authentication.....	3-3
Retributing Unauthorized Logon Attempts.....	3-4
R/3 Authorization Concept	3-5
Authority Checks	3-5
Profile Generator.....	3-6
Authorization Infosystem.....	3-7
Network Communications	3-8
SAProuter.....	3-8
Secure Network Communications (SNC)	3-9
Secure Store & Forward (SSF) Mechanisms and Digital Signatures	3-11
Public-Key Technology	3-11
Auditing and Logging.....	3-15
The Audit Info System (AIS).....	3-15
The Security Audit Log.....	3-16
R/3 Internet Applications Security.....	3-17
CHAPTER 4: CUSTOMER SERVICES	4-1
Security Consulting Team.....	4-1
SAP Audit User Group	4-3
Feedback Services.....	4-3

Table of Figures

Figure 4-1: An Overview of R/3 Security Services.....	3-1
Figure 4-2: Passwords	3-2
Figure 4-3: Single Sign-On	3-3
Figure 4-4: Generating Profiles using the Profile Generator.....	3-6
Figure 4-5: The Authorization Infosystem.....	3-7
Figure 4-6: SAProuter	3-8
Figure 4-7: Network Area Protected with SNC	3-10
Figure 4-8: Digital Signature	3-12
Figure 4-9: Digital Envelope.....	3-13
Figure 4-10: The Internet Transaction Server.....	3-17
Figure 4-11: Providing ITS Security	3-18

How to Use the R/3 Security Guide

The *R/3 Security Guide* consists of three separate volumes, with different levels of detail:

R/3 Security Guide VOLUME I : An Overview of R/3 Security Services

R/3 Security Guide VOLUME II : R/3 Security Services in Detail

R/3 Security Guide VOLUME III : Checklists

R/3 Security Guide VOLUME I : An Overview of R/3 Security Services

The *R/3 Security Guide VOLUME I* provides a general overview of the security services that we offer in R/3. With *VOLUME I*, you can familiarize yourself with these services, for example, before establishing a security policy or before installing an R/3 System.

R/3 Security Guide VOLUME II : R/3 Security Services in Detail

This part of the *R/3 Security Guide* concentrates on the technical measures involved with R/3 System security. It contains descriptions of the tasks involved, as well as our recommendations for the various components of the R/3 System. Use *VOLUME II* once you have established a security policy and are ready to implement it for your R/3 System.

R/3 Security Guide VOLUME III : Checklists

The third part of the *R/3 Security Guide* complements *VOLUME II* with checklists. You can use these checklists to record those measures that you have taken and for assistance when reviewing and monitoring them.

Updates

We will also publish updates to the guide as necessary. These updates will also be available over SAPNet in regular intervals.

Valid Releases

This version of the *R/3 Security Guide* applies to R/3 Releases 3.0, 3.1, and 4.0. Where applicable, references to other releases are explicitly indicated.

Typographical Information and Standard Notations

The following tables explain the meanings of the various formats, symbols, and standard notations used in the guide.

Table 1: Typographical Information Used in this Guide

This text format	helps you identify
<i>Screen Text</i>	words or characters you see on the screen (this includes system messages, field names, screen titles, menu names, and menu items).
User Entry	exact user input. These are words and characters you type on the keyboard exactly as they are in the documentation.
<Variable User Entry>	variable user input. Pointed brackets indicate that you replace these variables with appropriate keyboard entries.
ALL CAPITALS	report names, program names, transaction codes, table names, ABAP language elements, file names, and directories.
<i>Book Title</i>	cross-references to other books or references.
KEY name	keys on your keyboard. Most often, function keys (for example, F2 and the ENTER key) are represented this way.
Technical Object Name	names of technical objects outside of the R/3 System (for example, UNIX or Windows NT filenames or environment variables).
This icon	helps you identify
 Example	an Example. Examples help clarify complicated concepts or activities.
 Note	a Note. Notes can contain important information like special considerations or exceptions.
 Caution	a Caution. Cautions help you avoid errors such as those that could lead to data loss.

Chapter 1: Introduction

With the increasing use of distributed systems to manage business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply likewise to the SAP R/3 System. Therefore, at SAP, we offer a number of services to meet the security demands on the R/3 System.

However, to effectively use our services, you need to make your own contribution as well. You need to determine which security demands apply specifically to your system. We encourage you to carefully analyze your requirements on system security and define priorities. Where are you most vulnerable? What information do you consider critical? Where is critical information stored or transferred? What security options are available to protect your critical data and communications?

We recommend you establish a **security policy** that reflects these requirements and priorities. Your security policy needs to be supported and encouraged from upper management as well as from your employees. It should be practiced company-wide and cover your entire IT-infrastructure, to include your R/3 System. It should encompass all security aspects that are important to your system. Security aspects that you could consider include:

- User Authentication
- Authorization Protection
- Integrity Protection
- Privacy Protection
- Proof of Obligation (non-repudiation)
- Auditing and Logging

To enforce your security policy and meet your security requirements on the R/3 System, we offer a variety of **R/3 Security Services** based on these aspects. Our services include:

- **User Authentication**
 - R/3 Password Rules
 - Single Sign-On / Smart Card Authentication
 - Retributing Unauthorized Logon Attempts
- **R/3 Authorization Concept**
 - Authority Checks
 - Profile Generator
 - Authorization Infosystem
- **Network Communications**
 - SAProuter
 - Secure Network Communications (SNC)

Chapter 1: Introduction

- **Secure Store & Forward (SSF) Mechanisms and Digital Signatures**
- **Auditing and Logging**
 - The Audit Info System (AIS)
 - The Security Audit Log
- **R/3 Internet Applications Security**

We have designed our services to give you an individual and flexible approach to R/3 security. Depending on your priorities, you may decide to use some or all of these services.

We provide the *R/3 Security Guide* to assist you when using our services with the R/3 System. In this volume of the guide you receive an overview of our services that relate to security. See the *R/3 Security Guide VOLUME II: R/3 Security Services in Detail* for a detailed description on how to configure and administer the various components of the R/3 System that are relevant to security. *VOLUME III* complements *VOLUME II* with checklists.

Keep in mind that the most important factor in providing system security is your own security policy! This guide is intended to assist you when implementing a security policy, but it cannot replace your own investment of time and assets. We recommend you dedicate sufficient time and allocate ample resources to implement your security policy and to maintain the level of security that you desire.

Chapter 2: Security Aspects

When establishing your security policy, you need to decide what information or processes you consider critical. You need to decide what type of protection you need for this information. Your security policy should encompass aspects such as:

- **Authentication**

It is important to only allow legitimate users access to your system and prevent users from being impersonated!

- **Authorization**

It is important that users can only perform tasks for which they are authorized!

- **Integrity**

It is important that data cannot be changed without detection!

- **Privacy**

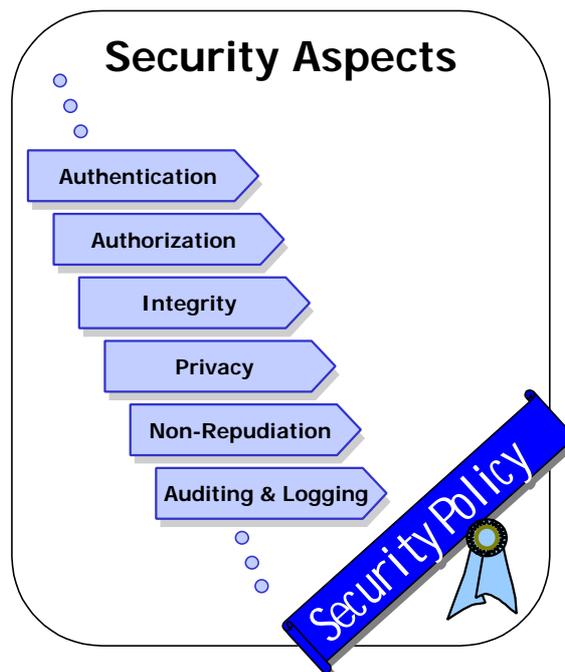
It is important to protect data or communications from unauthorized viewing or eavesdropping!

- **Obligation (non-repudiation)**

It is important to be able to ensure liability and legal obligation!

- **Auditing and Logging**

It is important to record activities and events for future references (for example, audits)!



We describe these aspects in more detail below.

Authentication

A basic, necessary security task is to make sure that users and information in a system are authentic. You need to know that the users who operate within your system are known users and that they cannot be impersonated. We offer several mechanisms in R/3 to protect user accounts from being misused. As a standard practice, R/3 authenticates its users by using passwords. The R/3 System has a number of built-in password rules that you can also expand on to meet your needs. For example, you can force users to regularly change their passwords, or you can prohibit certain words or character combinations. R/3 also locks users and sessions after a number of unsuccessful logon attempts to prevent unauthorized users from gaining access to the system. If you have additional requirements, you can use our Secure Network Communications (SNC) to provide authentication outside of the R/3 System. For example, with SNC you can establish a Single Sign-On environment or use smart cards for authentication. (For more information, see the section titled *User Authentication*.)

Authorization

It is important that users can only perform those tasks for which they are authorized. A typical company has various roles in its organization, and the personnel who fill these roles perform certain tasks. Data and processes should not be accessible by roles where they are not needed. For example, a worker in the personnel department needs access to payroll processes and employee data. This information should not be accessible to workers in other departments such as manufacturing or sales.

The R/3 authorization concept provides for protection against unauthorized access. Users can only use those transactions and programs that they are explicitly allowed to access. When a user attempts to run a transaction or program, R/3 performs an authority check before allowing access to the user. If the user does not have the proper authorizations, then R/3 denies the user's access request to the corresponding programs or transactions.

The **Profile Generator** and the **Authorization Infosystem** are available to assist you when working with the R/3 authorization concept. The Profile Generator provides a top-down approach to assigning authorizations and the Authorization Infosystem provides you with an easily accessible overview about your authorizations and their assignments.

Integrity

You need to protect the information that you process on a daily basis from unauthorized changes, either through error or deliberate acts. If a user processes a transaction (for example, makes a payment on an account), he or she needs to be sure that the information remains consistent throughout processing. When a user accesses data, he or she needs to be sure that it is the data that was last saved. The hardware and software must operate according to expectations, without executing undefined or unwanted actions. This process must function so well that the system as a whole can function without problems or without corrupting the data.

The following are examples of some of the mechanisms used or available in R/3 to provide integrity protection:

- R/3 protects data integrity at the database level using a locking mechanism.
- The presentation software performs an integrity check on itself to make sure that it does not contain viruses.
- Digital signatures are available with the Secure Store and Forward (SSF) mechanisms and are used by certain applications. Digital signatures not only prove the identity of the 'signer', but can also be used to verify the integrity of a signed data packet.
- You can use SNC and an external security product with R/3 to provide integrity protection for data communications between R/3 components.
- R/3 also logs all imports and exports to and from the system.

Privacy

It has always been necessary to protect sensitive and private information from viewing by unauthorized parties. For example, when you exchange personal information, you mark it as "confidential". Employers are obligated to keep contracts and employee information secret. Data protection laws prohibit distributing personal information. Company and customer information, or product and prototype information are kept in a company safe. This protection also applies to data that is saved on or communicated over electronic media.

The R/3 authorization concept makes sure that users are only allowed to access the data that they need. To apply privacy protection to the R/3 data communications, you can use SNC to encrypt the data that is transferred between R/3 components. Our SSF mechanisms also use encryption to "wrap" data in secure formats, called **digital envelopes**, before the data is transmitted or saved.

Obligation (non-repudiation)

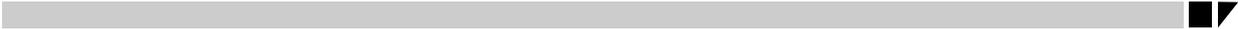
The proof of obligation (non-repudiation) in reference to electronically saved or transmitted data is indispensable in electronic commerce. A message is considered obligatory if you can guarantee who the creator of the message is, as well as the correctness of the message. Only so can electronic commerce establish itself in today's business world. For example, before closing an electronic (paperless) contract, you want to be sure that the contract is obligatory and proof-worthy. Therefore, it must be possible to prove the authenticity of the sender of the document, as well as the actuality of its contents.

Using the SSF mechanisms, certain applications in R/3 use **digital signatures** to enforce non-repudiation. In these application areas, handwritten signatures are replaced with digital signatures, automating the work processes while maintaining one-to-one identification of the signer at the time of signing. The following are examples of applications that currently use SSF to produce digital signatures (as of Release 4.0):

- Quality Management
- Product Data Management
- Production Planning for Process Industries

Auditing and Logging

It is also important to record events and activities for future reference. It is not only necessary to save certain information for legal purposes – logs and audits can also prove to be indispensable in monitoring the security of your system and tracking events in case of problems. R/3 keeps a variety of logs for system administration, monitoring, problem solving and auditing purposes. The **Audit Info System** and the **Security Audit Log** are the auditing tools that we include as part of the R/3 security services. Additional logs include the system log, statistic records in CCMS (Computing Center Management System), change documents for business objects, and application logging.



Chapter 2: Security Aspects

Chapter 3: The R/3 Security Services

In the last chapter, we described the security aspects of authentication, authorization, integrity, privacy, non-repudiation, and auditing and logging. Our R/3 security services are available to provide protection based on these aspects. Figure 3-1 shows an overview of our R/3 security services.

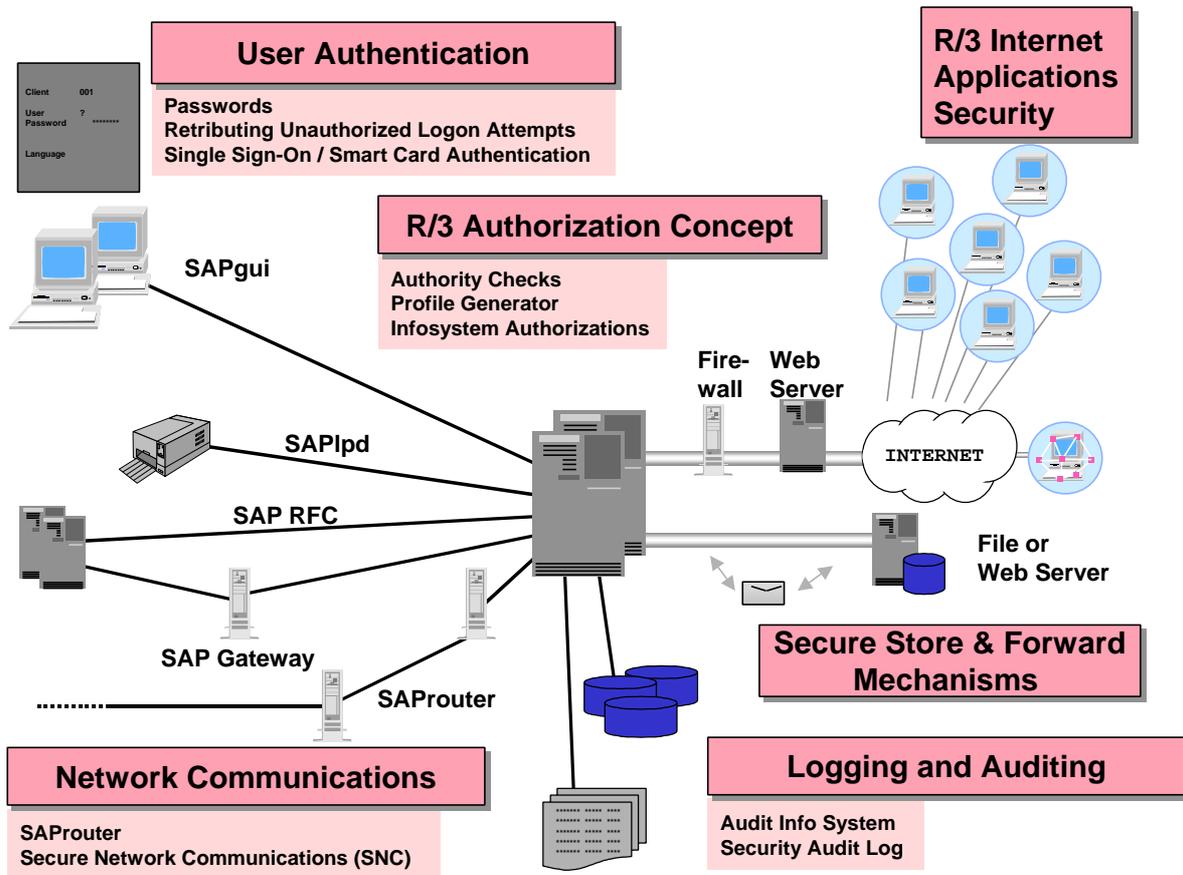


Figure 3-1: An Overview of R/3 Security Services

The individual services are described in more detail in the sections that follow.

User Authentication

The R/3 System comes with its own user management service. For each user, the R/3 System maintains an individual account, called a user master record, that contains all of the information that is specific to the user (for example, user-id, password, and authorizations).

To authenticate its users, the R/3 System uses **passwords** as its standard mechanism. You can also use an external security product with R/3 to provide for authentication outside of the R/3 System. By using an external product with R/3, you can use features such as **Single Sign-On** or **smart card authentication**. In addition, R/3 retributes **unauthorized logon attempts** with user and session locks. These mechanisms are described in more detail below.

R/3 Password Rules

We provide a set of standard rules for passwords in R/3. You can adjust many of these rules in profile parameters to meet your own security policy requirements.

The standard passwords rules include:

- First time dialog users receive an initial password that they must change when used for the first time.
- The default minimum length for passwords is 3. (You can increase this value in a profile parameter.)
- The maximum length is 8.
- The first character cannot be '?' or '!'.
• The first three characters cannot appear in the same order as part of the user name.
- The first three characters cannot all be the same.
- The first three characters cannot include space characters.
- The password cannot be PASS or SAP*.
- You cannot reuse the last five passwords.
- A user can only change his or her password when logging on.
- You can force users to have to change their passwords on a regular basis.
- You can prohibit certain words or character patterns.



Figure 3-2: Passwords

Single Sign-On / Smart Card Authentication

If you use our Secure Network Communications and an external security product (see the section titled *Network Communications*), you can make use of a **Single Sign-On** environment. The Single Sign-On environment must be established by an external security product; SNC uses this environment.

With Single Sign-On, your users only have to authenticate themselves once, even if they work on several systems. They logon to an external security product; the security product creates "credential" information for the users that it then provides to further systems such as R/3. When a user accesses a system that is protected by the security product, for example an R/3 System, he or she is automatically logged on to the system based on the authentication information that it receives from the product (see Figure 3-3). The product does not send any password information over the network; it sends a verification that it has authenticated the user.

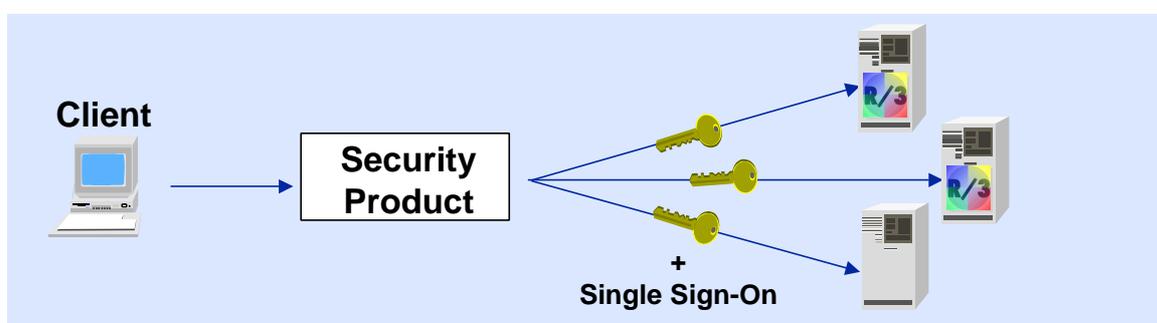


Figure 3-3: Single Sign-On

SNC provides more than just Single Sign-On; it also provides additional integrity and privacy protection for data communications. To provide its protection, SNC requires the use of a SAP-certified external security product. For a "Single Sign-On only" environment under Windows NT, you can use the Microsoft NTLMSPP (NT LAN Manager Security Support Provider) as the security provider. With this solution, you do not need to purchase a SAP-certified product. See OSS Note 138498 [2] and the *SNC User's Guide* [10] for more information.

Depending on the security product that you use with SNC, you may also be able to use **smart cards** for authentication purposes. (You need an external security product to be able to use smart cards, and not all security products support them.) With smart cards, the user's authentication information is stored on his or her personal card. Such cards are also often protected with a PIN (Personal Identification Number). Because the user has **possession** of the card as well as **knowledge** of the PIN, the chance of someone copying or confiscating the information is greatly reduced. Once again, with smart card authentication, it is no longer necessary to transfer password information over the network.

Note

Although authentication takes place outside of the R/3 System with Single Sign-On, authorization protection still occurs within R/3.

Retributing Unauthorized Logon Attempts

In addition to authenticating users at logon, R/3 retributes unauthorized logon attempts with the following mechanisms. You can also adjust most of these mechanisms in profile parameters to meet your own security policy requirements.

- R/3 terminates the session if a number of unsuccessful logon attempts occurs under a single user-id.
- R/3 locks a user-id after a number of unsuccessful logon attempts.
- R/3 can automatically log-off idle users.

For additional protection, we suggest that you:

- Require your users to use screen savers with passwords.
- Regularly monitor your system and check for unauthorized logon attempts.

R/3 Authorization Concept

The R/3 authorization concept protects transactions and programs from unauthorized use. R/3 does not allow users to execute transactions or programs for which they do not have explicitly defined authorizations. You decide which programs and transactions users are allowed to call and assign them the appropriate authorizations in the user master records. When a user starts a program or calls a transaction, R/3 performs **authority checks** to make sure that the user has the proper authorizations.

To assist you in working with the R/3 authorization concept, we also offer the **Profile Generator** and the **Authorization Infosystem** as part of our R/3 security services.

Authority Checks

To enforce the R/3 authorization concept, R/3 performs authority checks when users attempt to execute programs or transactions. In the authority checks, R/3 makes sure that the user has the appropriate authorizations in his or her user master record before allowing the user to proceed. There are various types of authority checks which include:

- **R/3 Start Transaction Authorization**

A user must have the appropriate authorization to start transactions. This applies to transactions that are started either over the menu or called over the command line.

- **Specific Authorization for a Transaction**

Besides the start transaction authority check, SAP transactions are protected with additional authority checks. When you create your own transactions, you can also assign additional authority checks. One method is to assign a specific authorization for the transaction. This is useful if you can protect the transaction with a single authorization. If this is not the case, there are other methods also available.

- **AUTHORITY-CHECK at program level**

Another method of assigning additional authority checks is to include an AUTHORITY-CHECK at the program level. In this way, you can protect individual programs at the code level. SAP programs use this method for protection and we highly encourage you to use it for your own developments as well.

- **Report Classes and Table Authorization Groups**

In addition to program or transactional authority checks, you can assign reports to report classes and authorization groups to tables. Although users may be able to use the transactions to run reports or access tables, they can only access those reports and tables for which they have the corresponding authorizations.

Profile Generator

The profile generator makes your job easier by automating certain processes and providing more flexibility in your authorization assignments. The central idea is to take a step away from the technical aspects of authorizations and authorization objects and to configure your authorization assignments according to job roles, activity groups, and tasks.

The profile generator uses a top-down approach for generating authorization assignments. You start with your company menu and work your way down to the individual user master records. You define your job role model, create activity groups and decide which transactions and functions each role needs to use. The profile generator handles the rest - including the selection of the authorization objects needed for the various tasks. This process is shown and briefly described in Figure 3-4.

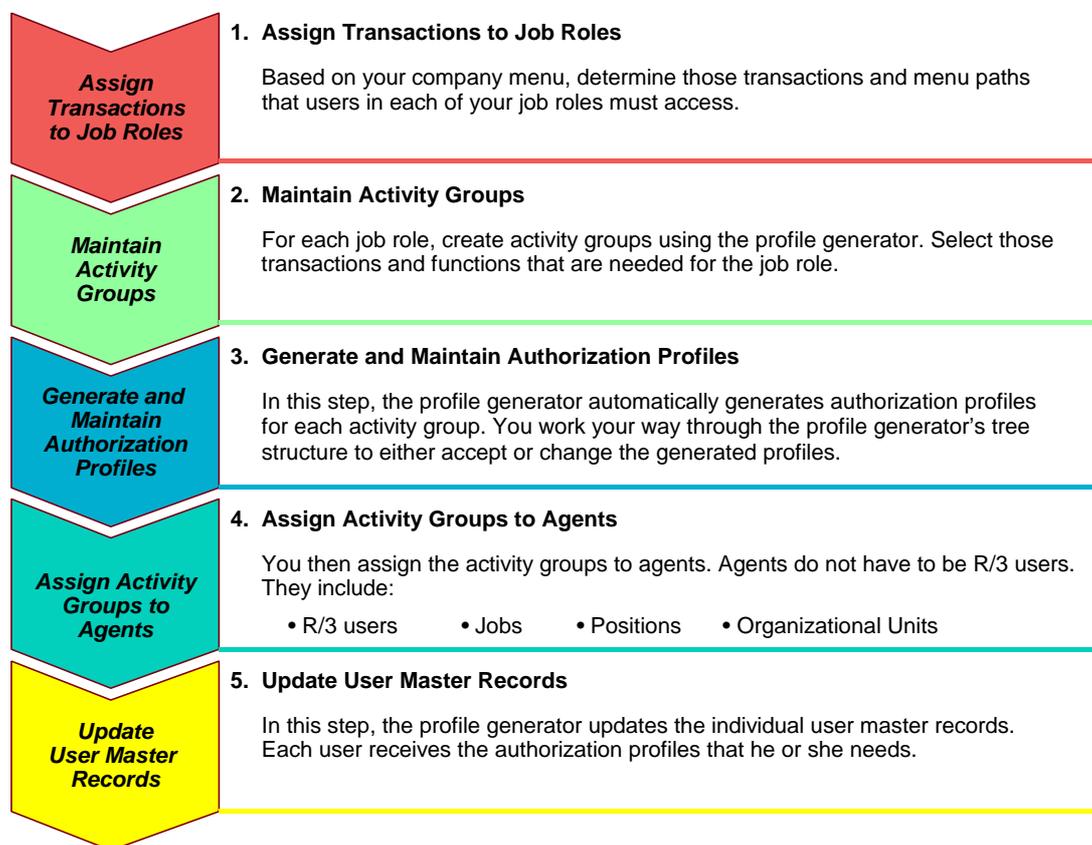


Figure 3-4: Generating Profiles using the Profile Generator

With the profile generator, you have a flexible approach with a degree of automation that makes your job of administering authorizations much easier. We encourage you to use the profile generator to maintain your users' authorizations.

Availability

The profile generator is available as part of the standard delivery with Release 3.1G and runs on all supported platforms.

Authorization Infosystem

You can use the Authorization Infosystem to obtain an overview of your authorizations, profiles, users, and authorization assignments. With the Authorization Infosystem you can quickly and easily obtain the information you need from your R/3 System.

The Authorization Infosystem is a reporting tree (similar to the Implementation Guide). You can use it to generate a number of lists to include:

- Users with certain authorizations
- Authorizations that a certain user has
- All authorizations
- Profile comparisons
- Transactions that a user can execute
- Changes in the authorization profile for a user

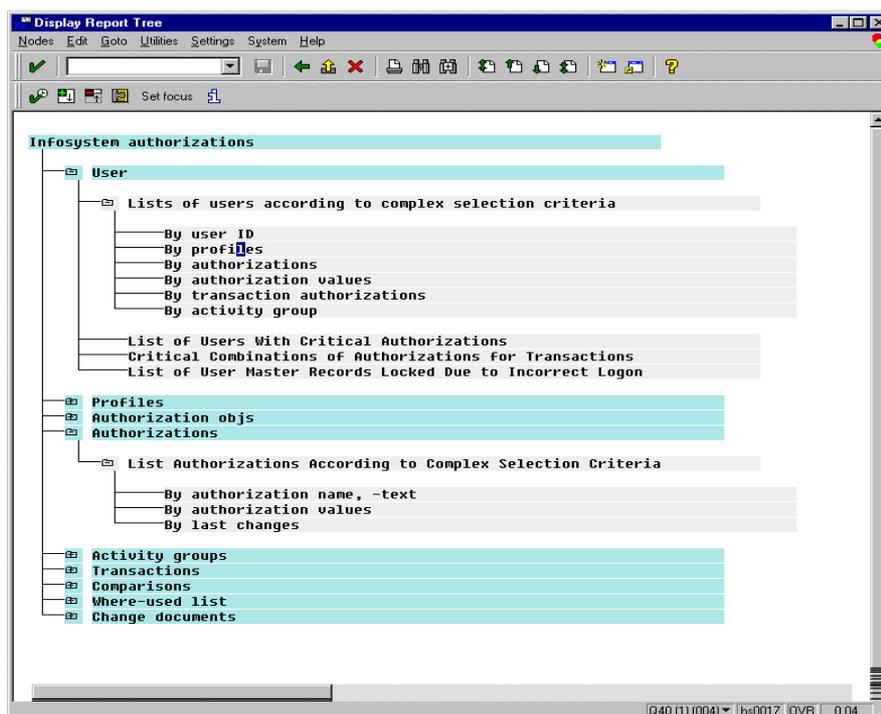


Figure 3-5: The Authorization Infosystem

With the Authorization Infosystem, you have a quick and easily accessible source of information about your users and your authorization assignments.

Availability

The Authorization Infosystem is also available as of Release 3.1G.

Network Communications

Your network infrastructure is extremely important in regard to your system security. You need to be able to support your communication needs without allowing for unauthorized access to your network. If you design your network topology with security as a priority, you can reduce many possible threats.

Again, your strategy and priorities are the most important factors when deciding what level of network security you consider necessary. We do offer general recommendations when establishing your network topology, and we recommend contacting our Security Consulting Team for further assistance if necessary (see *Chapter 4: Customer Services*).

Our main R/3 security services that we provide for network security are the **SAProuter** and **Secure Network Communications (SNC)**.

SAProuter

The SAProuter is an application-level proxy that you can use together with a firewall to effectively protect your network from unauthorized access. You use a firewall to prohibit unwanted access to your internal network. For those communications that you do want to accept, you need to open corresponding 'doors' in the firewall where the communication requests are allowed to pass through. You can then use the SAProuter as a 'guard' behind these doors to further control access within your network. The SAProuter also makes sure that the request is valid, but at a more detailed level. The SAProuter can accept or deny requests coming from a specific user or machine, or it can direct a request to a specific machine only. By using the SAProuter together with a firewall, you can effectively protect your R/3 System LAN from unauthorized access.



Example

In Figure 3-6, the firewall denies all `telnet` requests and the request from User Z is blocked. However, the firewall is open for the SAP protocol `DIAG`, which is used for SAPgui connections. The SAProuter is then used to make sure that only certain users can access the R/3 System LAN using `DIAG`. The `DIAG` requests from both User X and User Y are accepted by the firewall, but the SAProuter only accepts the request from User Y.

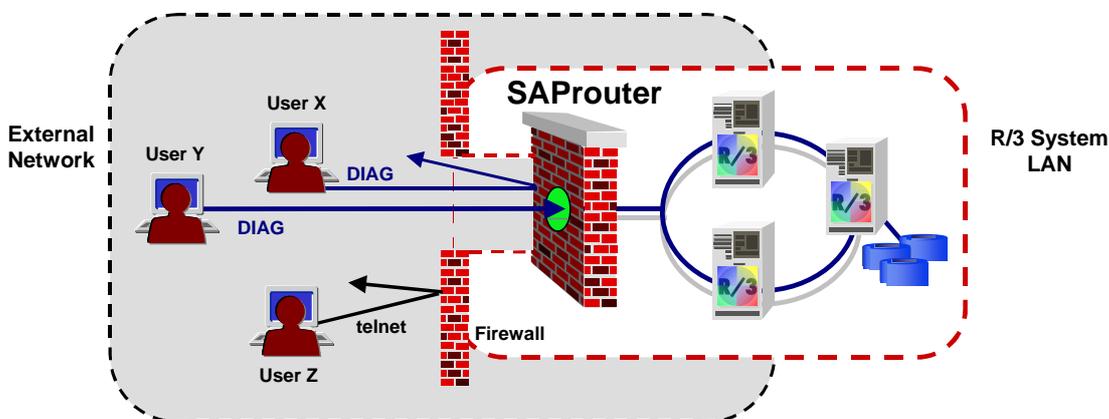


Figure 3-6: SAProuter

**Note**

The SAProuter alone does not suffice to control access to your network. You need to use it in combination with a firewall system!

You can use SAProuter to:

- Control and log the connections to your R/3 System, for example, from an SAP service center.
- Set up an indirect connection when programs involved in the connection cannot communicate with each other due to the network configuration.
- Improve network security by
 - Protecting your connection and data from unauthorized external access with a password.
 - Allowing access from only particular SAProuters.
 - Only allowing encrypted connections from a known partner (when using SNC).
- Increase performance and stability by reducing the R/3 System load within a local area network (LAN) when communicating with a wide area network (WAN).

**Note**

Although the SAProuter and firewall combination is often used to separate an internal network from external networks, we highly recommend that you use it to control access between different internal networks as well!

**Note**

If you are using the R/3 Online System Services, you **must** use a SAProuter!

Secure Network Communications (SNC)

SNC provides protection for the communications between the distributed components of the R/3 System. Each R/3 component contains a software layer, called the SNC layer, that enables R/3 to integrate with an external security product. R/3 communicates with the external product using the standard interface GSS-API V2 (Generic Security Services Application Programming Interface Version 2). The GSS-API V2 was developed with SAP participation by the Internet Engineering Task Force (IETF).

The SNC option allows you to integrate an external security product with R/3 and use the product's security features that are not directly available in R/3. You can therefore choose the product that offers you the features that best meet your needs. Examples of features provided by security products include:

- Single Sign-On
- Smart card authentication
- Encryption of data streams between R/3 components (integrity and privacy protection)

Chapter 3: The R/3 Security Services

The external security product is not included with the SAP R/3 software. You must purchase the product from the appropriate vendor and it must be certified by SAP. For product support and availability, see the Complementary Software Program in SAPNet under the alias 'csp' (for example, <http://sapnet.sap-ag.de/csp>); then follow the link *Complementary Solutions* → *Network security*.

There are also laws in various countries that regulate the use of cryptography in software. You need to keep yourself informed on the impact these laws may have on your applications, and make sure that you are aware of any further developments.

Application-level Security

SNC provides security at the application level. This means that you are guaranteed secure communications between the two communication partners (for example, the R/3 application server and SAPgui), regardless of the transport medium.

SNC provides protection between R/3 application servers, clients, and SAProuters. However, you cannot apply SNC protection to the communication path between the application servers and your database. For this reason, we recommend that you keep your database and application servers in a secure LAN. Figure 3-7 shows those areas of your LAN or WAN that are secured by SNC.

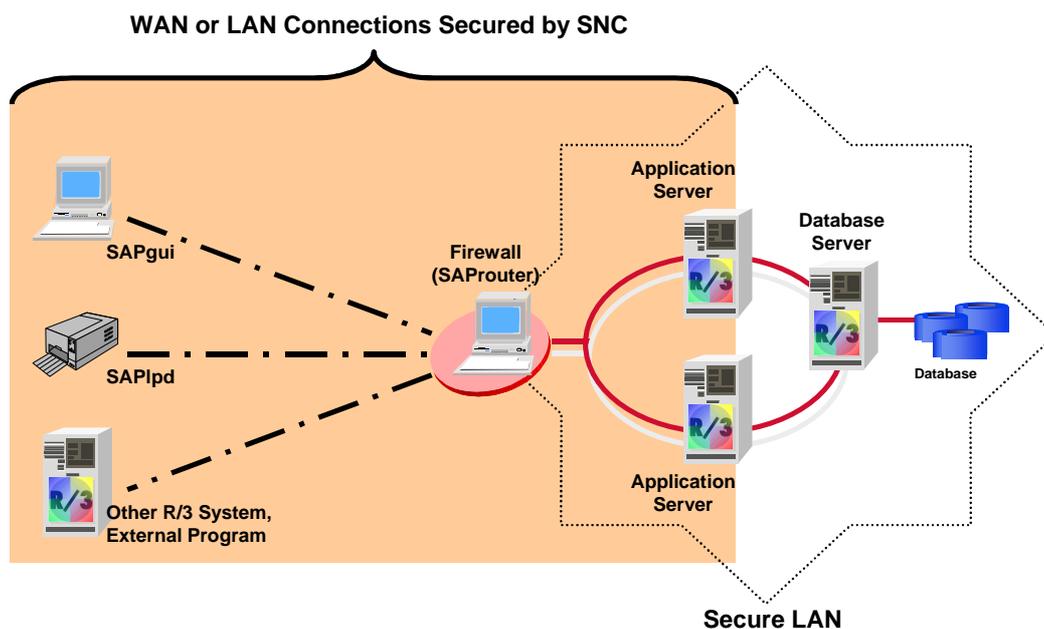


Figure 3-7: Network Area Protected with SNC

Availability

SNC protection is available for SAPgui and SAPIpd connections as of Release 3.1G and additionally for remote communication connections (RFC and CPI-C) as of Release 4.0. You can also use SNC protection to secure SAProuter communications as of SAProuter Version 30.

Secure Store & Forward (SSF) Mechanisms and Digital Signatures

As of Release 4.0, R/3 applications can use Secure Store & Forward (SSF) mechanisms to protect arbitrary data in the R/3 System. R/3 applications can use the SSF mechanisms to secure data integrity, authenticity and confidentiality. The data is protected even if it leaves the R/3 System. The first applications that use SSF include:

- Production Planning - Process Industry
- Product Data Management
- SAP ArchiveLink - SAP Content Server HTTP interface 4.5

With time, more and more applications will use SSF for their security purposes.

SSF requires the use of a security product to perform its functions. As of Release 4.5, R/3 is shipped with SAPSECULIB (SAP Security Library) as the default SSF service provider. SAPSECULIB is a software solution with functionality that is limited to digital signatures. For support of crypto hardware (for example, smart cards or crypto boxes) or digital envelopes, you need a SAP-certified external security product.



Note

There are also laws in various countries that regulate the use of cryptography and digital signatures. These laws are currently controversial and may change. You need to keep yourself informed on the impact these laws may have on your applications, and make sure that you are aware of any further developments.

Public-Key Technology

SSF uses **digital signatures** and **digital envelopes** to secure digital documents. The digital signature uniquely identifies the signer, is not forgeable, and protects the integrity of the data. Any changes in the data after being signed result in an invalid digital signature for the altered data. The digital envelope ensures that the contents of the data are only visible to the intended recipient.

Digital signatures and digital envelopes are based on public-key technology. A user who produces digital signatures or digital envelopes owns a pair of keys. These two keys have the following characteristics:

- The keys are a pair; they belong together.
- You cannot compute either of the keys from the other.
- As the name suggests, the public key is to be made public. A recipient of a signed document needs to have knowledge of this key to verify the digital signature, and the sender of a private document needs the recipient's public key to encrypt the document and hide its contents.

The owner of the keys distributes the public key as necessary. Typically, he or she owns a **public-key certificate** that contains all of the relevant information that he or she needs to distribute (for example, name, organization, his or her public key, the certificate's validity period and the organization that issued the certificate). To distribute the public key, he or she distributes the public-key certificate.

Chapter 3: The R/3 Security Services

- The private key is to be kept secret. The owner of the keys uses the private key to generate his or her digital signature. Therefore, the owner of the keys needs to make sure that **no** unauthorized person or system has access to his or her private key.

Digital Signatures

The private key is used to create the digital signature for a digital document. As long as the owner of the private key keeps it secret, nobody else can create an identical digital signature for the document.

Figure 3-8 shows how a digitally signed document is created. Note that generally, you indicate that you want to 'sign' a document and the system does the rest.



Note

To 'sign' a document, you need to give the system explicit access to your private key. For example, if your private key is stored on your smart card, then you must first provide a PIN or passphrase to allow the system access to your smart card.

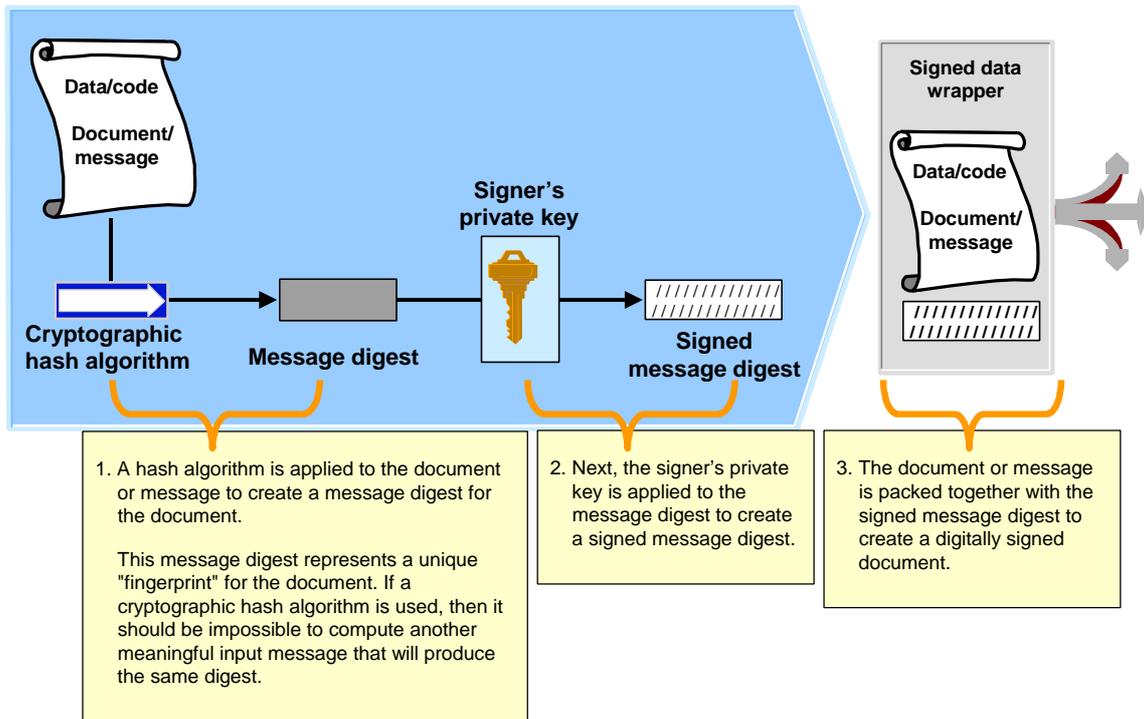


Figure 3-8: Digital Signature

Anyone with access to the signer's public key can reverse the transformation and retrieve the message digest from the signed message digest. To verify the authenticity of the digital signature, and the integrity of the data, the same hash function is applied to the document and the result is compared with the message digest. If the two message digests are the same, then the digital signature is valid.

Only the public key that matches the private key that was used to sign will produce a positive verification of the digital signature. In addition, if any changes have occurred in the digital signature or in the document after being signed, then the verification will fail. In this way, a positive verification proves both the authenticity of the signer as well as the integrity of the document.

Digital Envelopes

You can use digital envelopes to ensure that only the intended recipients can read the contents of documents. To create a digital envelope, you use a secret message key to "wrap" the document in an "envelope". The recipient of the message also needs knowledge of this key to decrypt the document. Therefore, as part of the digital envelope, you encrypt the message key using the recipient's public key and send it along with the document. This process is shown in Figure 3-9.

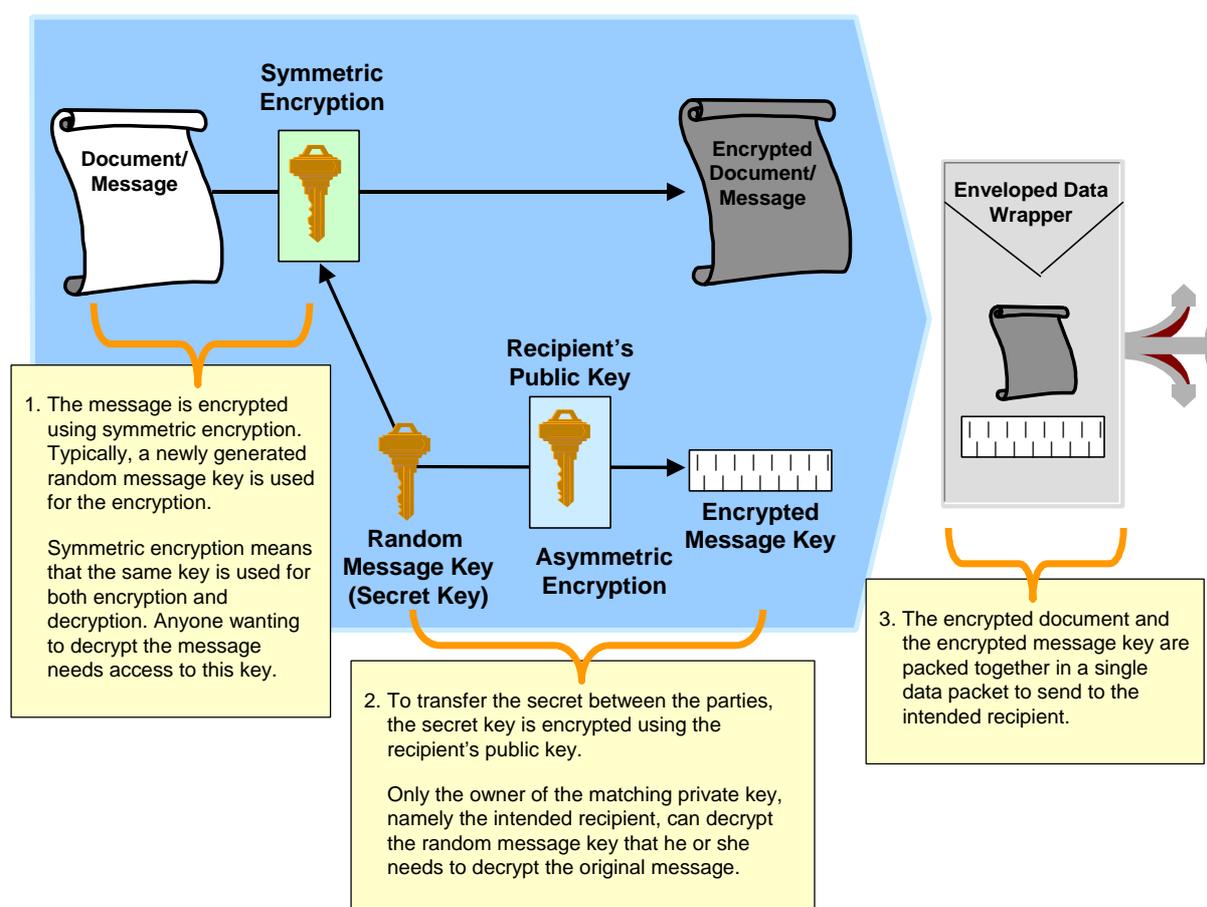


Figure 3-9: Digital Envelope

The recipient of the document uses his or her private key to decrypt the message key, which he or she can then use to decrypt the document.

Public-Key Infrastructure

To successfully use digital signatures and digital envelopes, a public-key infrastructure (PKI) must be established. The PKI generates and distributes the key pairs. Because there is not yet a worldwide PKI available, you have to either establish your own or rely on a Trust Center as a PKI service provider. Establishing your own local PKI for a very limited number of users only may or may not be easy, depending on the external security product that you use. Even if establishing a local PKI is easy, the process of linking the PKI to your customers and business partners may involve a much greater effort. By agreeing on a common Trust Center, you and your partners can reduce many of the PKI problems.

Application Scenarios

The SSF functions can be applied in various scenarios for protecting data and documents. You can use digital signatures to sign various types of 'paperless' documents such as payment requests, purchase orders, or contracts. Typical application scenarios in R/3 include:

- The application that uses SSF converts the plain text data from the SAPgui into the secure format and saves it in the R/3 database. When the application accesses the data at a later time, it reads the data from the database and decrypts it, also using the SSF functions. If the data has been signed with a digital signature, the application can also verify the digital signature.
- The application reads data from the R/3 database and prepares it for external transport or storage. To do this, it first converts the data to the corresponding external format and then secures the data using the SSF functions. Once the data exists in the secure format, the application can save it safely on a storage medium (for example, on disk or in an archive), or transmit it over (possibly) insecure communication lines (such as the Internet). The intended recipient can be another R/3 System, or a different system that supports the secure format used.
- The application received secured or digitally signed data from an external source and imports it into the R/3 System. If the data is secured using an SSF compatible format, then the application can use the SSF functions to decrypt it or verify the signature. Note that the data does not have to have been secured by an R/3 System, but it does need to use a format that is supported by SSF.

External Security Products

SSF also uses an external security product to provide protection. It uses the PKCS#7 standards and X.509 certificates for signing and encrypting data. The security product that you use for SSF must support these standards.

The external security product is not included with the SAP R/3 software. You must purchase the product from the appropriate vendor and it must be certified by SAP. For more information on using digital signatures in R/3, see OSS Note 86927 [14].

Availability

SSF mechanisms (digital signatures and digital envelopes) are available as of R/3 Release 4.0. The SAPSECULIB is available as of Release 4.5.

Auditing and Logging

Auditing and logging are also important aspects related to security. Not only is it necessary to save certain information for legal purposes – audits and logs can also prove to be indispensable in monitoring the security of your system and tracking events in case of problems. R/3 keeps a variety of logs for system administration, monitoring, problem solving and auditing purposes. We include the **Audit Info System** and the **Security Audit Log** as part of the R/3 security services.

Additional logs include the system log, statistic records in CCMS (Computing Center Management System), change documents for business objects, and application logging. Although we have not included these logs in the following description, you can find information on them in the *R/3 Security Guide: VOLUME II*.

The Audit Info System (AIS)

The Audit Info System (AIS) is an auditing tool that you can use to analyze security aspects of your R/3 System in detail. AIS is a tool aimed for auditors working in:

- Internal or external auditing
- System auditing
- Data security

Both business and system audits are available. Auditors and system administrators can use AIS to check the security of the R/3 System. Some of the types of audits where AIS is useful include:

- Ongoing controlling
- Interim audits
- Real-time auditing of your productive system

AIS presents its information in the Audit Info Structure (similar to IMG) so that you can easily determine which activities you need to perform and which you have accomplished. It uses a process-oriented, top-down approach so that you can access summarized data down to individual documents. Auditors work with AIS directly online in a productive system, thereby receiving real-time information.

Availability

AIS is available as a standard component as of Release 3.1I and 4.6. You can also import it into other releases (as of 3.0D). For more information on the availability of AIS see the OSS Notes 77503 [15] and 100609 [16].

The Security Audit Log

You can use the Security Audit Log to record security-related system information such as changes to user master records or unsuccessful log-on attempts. This log is also a tool designed for auditors or system administrators who need to take a detailed look at what occurs in the R/3 System. By activating the Security Audit Log, you keep a record of those activities that you specify for your audit. You can then access this information for evaluation in the form of an audit analysis report.

The Security Audit Log provides for long-term data access. The audit files are retained until you explicitly delete or archive them. Currently, the Security Audit Log does not support the automatic archiving of the log files; however, you can manually archive them at any time.

You can record the following information in the Security Audit Log:

- successful and unsuccessful dialog log-on attempts
- successful and unsuccessful RFC log-on attempts
- RFC calls to function modules
- changes to User Master Records
- successful and unsuccessful transaction starts
- changes to the audit configuration

Availability

The Security Audit Log is available as of Release 4.0.

R/3 Internet Applications Security

R/3 Internet Application Components (IAC) enable users to perform business functions in R/3 using a World Wide Web browser as the user interface instead of SAPgui.

We supply a number of IACs that you can use as they are, or you can modify them to meet your own needs. For example, you can configure the Web user interface to suit your corporate identity. In addition, you can also develop your own Internet Application Components.

The Internet Transaction Server (ITS) serves as the link between the R/3 System and the Web. It allows for effective communication between the two systems, in spite of their technical differences.

ITS Architecture

The design of the ITS provides for secure R/3 Internet applications. It acts as a stepping-stone between the Web Server and the R/3 application server. It controls the data flow between the R/3 System and the Internet and provides access to the Internet Application Components.

The ITS is composed of two components, the WGate and the AGate. The WGate is actually located on the Web Server and is used to connect the Web Server to the ITS. The AGate is generally located on a separate server and is responsible for the communication between the ITS and R/3. It establishes the connection, generates the HTML documents, and manages the session context and logon data.

This set-up is shown in Figure 3-10.

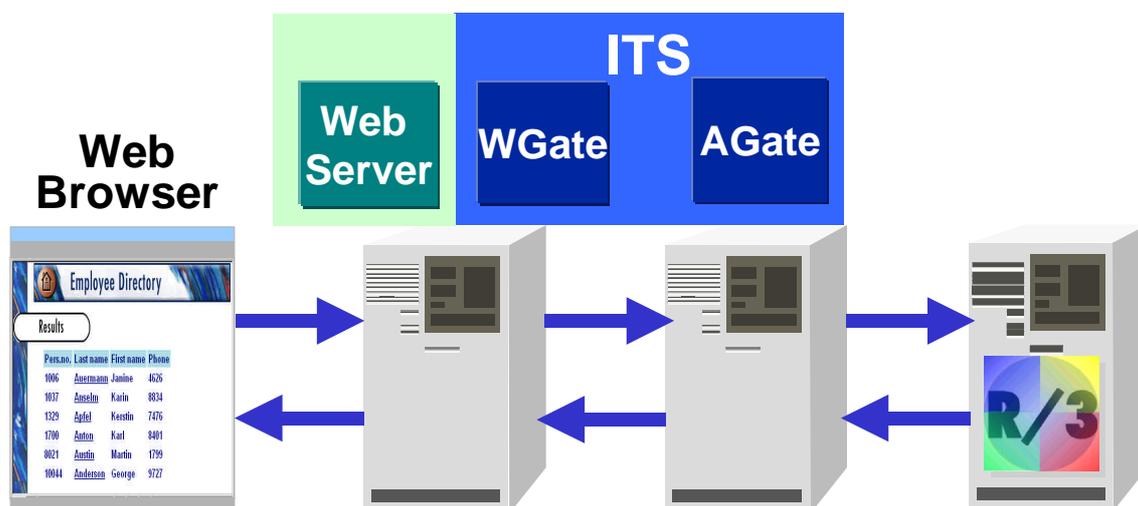


Figure 3-10: The Internet Transaction Server

Chapter 3: The R/3 Security Services

The R/3 Internet architecture has many built-in security features, such as the possibility to run the WGate and AGate on separate hosts. We strongly recommend that you set up a network infrastructure that makes use of these features to control access from the Internet to internal networks. We also recommend you use other security components, such as firewalls, packet filters and SAProuters to separate the individual parts of the network from another. Figure 3-11 shows some of the components that you can use to build a secure network architecture when using ITS.

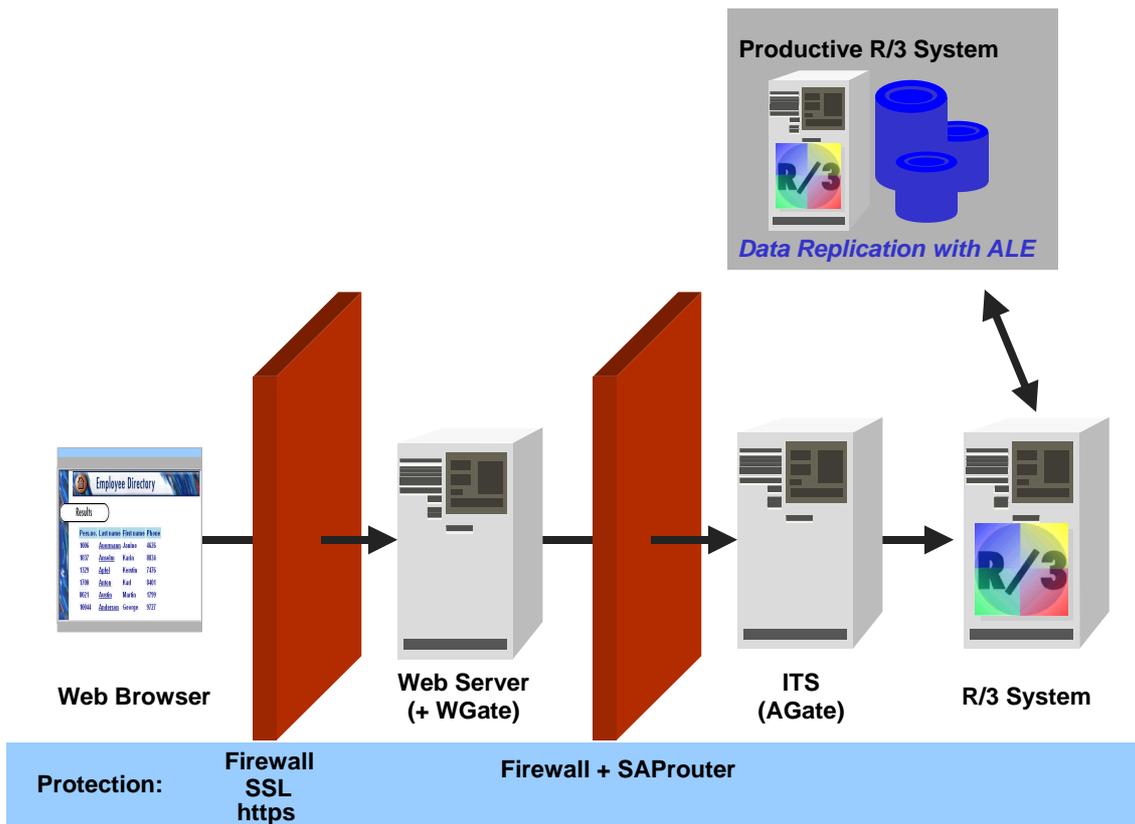


Figure 3-11: Providing ITS Security

You may decide to implement some or all of these components depending on your security policy.

 **Note**

To improve performance and reduce the amount of data available to your Internet applications, we recommend that you use a separate system (replicated using Application Link Enabling) for your "Internet" system, instead of your productive system.

Using Security Services / Providing Privacy

All data is usually transmitted through the Internet in simple plain text. To maintain confidentiality for this data, you can apply encryption. The following encryption methods are possible when using the ITS:

- **Between the Web Browser and Web Server:**
 - Secure Sockets Layer protocol (SSL)
- **Between the WGate and the AGate:**
 - ITS 1.0 and 1.1: static key
 - ITS 2.0: SNC
- **Between the AGate and R/3:**
 - SNC (as of Release 4.5)

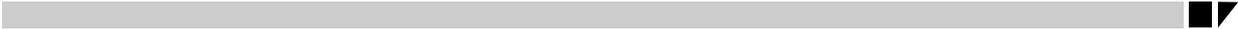
Availability

The ITS is part of the standard delivery as of Release 3.1G.

The WGate is compatible with the following Web Server interfaces:

- Microsoft's Information Server API (ISAPI) on Windows NT
- Netscape Server API (NSAPI) on Windows NT
- Common Gateway Interface (CGI) on UNIX and AS/400 (as of Release 4.5)

The AGate is available as a Windows NT service only.



Chapter 3: The R/3 Security Services

Chapter 4: Customer Services

We provide the R/3 security services and the *R/3 Security Guide* to assist you in analyzing and administering security in the R/3 System. In addition to these R/3 services, we offer special customer services related to security. These services include:

- The **Security Consulting Team** as part of the SAP Technical Consulting Services provides individual consulting services on security issues.
- The **SAP Audit User Group** has also published a number of guidelines that you can use for auditing your R/3 System.
- We also encourage you to use our **Feedback Services** to let us know how the R/3 Security Guide and the related security services meet your needs.

These customer services are described in more detail below.

Security Consulting Team

Creating, administering, and practicing an effective security policy involves various levels of expertise and know-how. To support you in establishing and enforcing your policy, our Security Consulting Team as part of the SAP Technical Consulting Services is available for assistance. The team provides in-depth expertise on security-related issues. If the *R/3 Security Guide* does not satisfactorily answer all of your questions, or if additional questions arise, then we encourage you to contact the Security Consulting Team for further assistance.

Our Security Consulting Team performs a variety of services to include analyzing your system in regard to security, assisting you when designing a security policy, introducing you to authorization concept techniques, and providing individual consulting on security-related issues.

The following services are available:

- **Comprehensive Security Analysis**

We perform a detailed security analysis of your R/3 Systems from a technical perspective. The analysis includes:

- Analyzing the technical system security at all levels (with emphasis on the R/3 Systems).
- Analyzing all security-relevant procedures.

- **Security Review**

We perform a security review on a single R/3 System from a technical perspective. The analysis includes:

- Analyzing the technical system security, restricted to critical areas.

(This check is limited to a single R/3 System.)

Chapter 4: Customer Services

- **Company-Specific Security Guide Support**

We provide support in designing and implementing your own, company-specific R/3 security guide. Our support includes:

- Analyzing security-relevant workflows.
- Developing procedures that promote security.
- Documenting the procedures in your company-specific security guide.
- Providing support during the implementation of your guide.

- **Workshop: Authorization Concept**

We help you plan an optimal implementation of the authorization concept. We explain:

- The authority checks and how they work.
- The tools for generating profiles.
- The conceptual procedure of assigning profiles during the implementation phase.
- The distribution of user management tasks.

- **NT Domain Concept**

We help you design a customer-specific NT domain concept for securing your operating system, database, and other resources. The contents include:

- Defining a user concept (user groups and access privileges).
- Creating implementation guidelines.
- Securing the integration of the R/3 environment in a Windows NT domain.

- **Training Course: CA900 Technical System Security**

We offer the training course CA900: Technical System Security. The contents of this course include:

- The security policy.
- The technical environment of the R/3 System.
- Access control in the R/3 environment.
- The development environment in R/3.
- The R/3 transport system.
- Security aspects in R/3 administration.
- The Internet Transaction Server (ITS).
- System audit tools.

- **Security Aspects when Using the Internet Transaction Server**

We explain all the security-relevant aspects that apply to the ITS to include:

- The architecture of the ITS.
- The integration of the ITS in an existing system landscape.
- Mechanisms for protecting the R/3 System and the ITS.
- Security-relevant aspects when configuring the ITS.

For further information, contact the Security Consulting Team in the Technical Consulting Department at:

Tel. **+49 6227 / 7-41537**
Fax: **+49 6227 / 7-44640**

SAP Audit User Group

The audit user group is a forum for the discussion of procedural and system audits performed on SAP installations and systems. The user group consists of auditors and IT-auditors that either audit SAP applications or whose companies use SAP software. Its purpose is to discuss user requirements and to review recommendations as to how to improve the use of SAP software.

The Audit User Group and its working parties have distributed the following guidelines and documentation for auditing SAP Systems:

- *SAP Audit Guideline R/2 RF*, Material Number 50019057 [22]
- *SAP Audit Guideline R/3 FI/MM*, Material Number 50014633 [23]
- *SAP Data Protection Guidelines R/3* (German only), Material Number 50024598 [24]
- *AIS Fact Sheet*, Material Number 50026092 [25]

In addition, we offer the training course AC900: Internal and External Auditing.

For more information on the SAP Audit User Group and the corresponding guidelines, see the link www.sap.com/germany/contact/user.htm and then choose *Arbeitskreis "Revision R/2 und R/3"*. [26]

Feedback Services

We are also interested in knowing how well the *R/3 Security Guide* meets your needs. If you have comments pertaining to the contents or quality of this guide, use the Feedback Reply Form provided at the end of the guide and return it to us at the following address or fax number:

SAP AG
CCMS & Security Department
Postfach 1461
D-69190 Walldorf
Germany

Fax: **+49-6227 / 7-41198**



Chapter 4: Customer Services

Appendix A: Additional Information

You can find additional information on the individual R/3 security services in the following documentation:



Note

For references to the R/3 online documentation, we have provided the locations for the Releases 3.1H and 4.0B. The menu paths may vary in other releases.

Table 2: Additional Information

Ref.No.	Description
User Authentication	
[1]	OSS Note 2467 : Answers on the topic of "Security"
[2]	OSS Note 138498 : Single Sign-On solutions
R/3 Authorization Concept	
[3]	SAP Documentation: Authorizations Made Easy Guide : Material Number 50020475 (Release 3.0F) Material Number 50021412 (Release 3.1G/3.1H) Material Number 50023994 (Release 4.0A/4.0B)
[4]	R/3 Online Documentation: BC Users and Authorizations Release 3.1H: <i>Basis Components</i> → <i>System Administration</i> → <i>Users and Authorizations</i> Release 4.0B: <i>BC - Basis Components</i> → <i>Computing Center Management System</i> → <i>BC Users and Authorizations</i>
[5]	Implementation Guide <i>Basis Components</i> → <i>System Administration</i> → <i>Users and Authorizations</i> → <i>Maintain authorizations and profiles using profile generator</i>
[6]	SAP ASAP Implementation Roadmap: Work-package 3.11 Establish Authorization Concept; Phase 3: Realization
Network Infrastructure	
[7]	BC SAProuter Release 3.1H: <i>R/3 Service and Support</i> → <i>SAProuter</i> Release 4.0B: <i>BC Kernel Components</i> → <i>BC SAProuter</i>
[8]	OSS Note 30289 : SAProuter documentation
[9]	SAP Documentation: Secure Network Communications and Secure Store & Forward Mechanisms with R/3 , Material Number 50014335
[10]	SAP Documentation: The SNC User's Guide , Presentations ITS CD in the directory <i>Docu</i> → <i>SNC</i> or see the SAPNet alias 'systemmanagement' (for example, http://sapnet.sap-ag.de/systemmanagement) and then <i>Media Center</i> → <i>Security</i> → <i>Literature</i>
[11]	OSS Note 66687 : Use of network security products
[12]	Complementary Software Program : See the alias 'csp' in SAPNet (for example, http://sapnet.sap-ag.de/csp) and follow the link <i>Complementary Solutions</i> → <i>Network security</i>

Table 2: Additional Information (continued)

Ref.No.	Description
Secure Store & Forward Mechanisms (SSF) and Digital Signatures	
[13]	<u>SAP Documentation</u> : <i>Secure Network Communications and Secure Store & Forward Mechanisms with R/3</i> , Material Number 50014335
[14]	<u>OSS Note 86927</u> : Use of the digital signature in the R/3 System
Auditing and Logging	
[15]	<u>OSS Note 77503</u> : Audit Information System (AIS) Version 1.5
[16]	<u>OSS Note 100609</u> : Audit Information System (AIS) - installation
[17]	<u>BC System Services → The Security Audit Log</u> Release 3.1H: not available Release 4.0B: <i>BC - Basis Components → Kernel Components → BC System Service → The Security Audit Log</i>
R/3 Internet Applications Security	
[18]	<u>R/3 Internet Application Components</u> Release 3.1H: <i>Cross Application → SAP@WEB → R/3 Internet Application Components</i> Release 4.0B: <i>CA - Cross-Application Components → Business Framework Architecture → Web Basis → R/3 Internet Application Components</i>
[19]	<u>OSS Note 60058</u> : Security for R/3 Release 3.1 on the Internet
[20]	<u>OSS Note 104576</u> : Package filter (firewall) between ITS and R/3
Related Guidelines	
[21]	<u>SAP Audit User Group</u> : See www.sap.com/germany/contact/user.htm and then choose <i>Arbeitskreis "Revision R/2 und R/3"</i>
[22]	<u>SAP Documentation</u> : <i>SAP Audit Guideline R/2 RF</i> , Material Number 50019057
[23]	<u>SAP Documentation</u> : <i>SAP Audit Guideline R/3 FI / MM</i> , Material Number 50014633
[24]	<u>SAP Documentation</u> : <i>SAP Data Protection Guidelines</i> , Material Number 50024598
[25]	<u>SAP Documentation</u> : <i>AIS Fact Sheet</i> , Material Number 50024598

Index

A

- AGate 3-17, 3-18, 3-19
- AIS See Audit Info System
- analysis, system (consulting services) 4-1
- aspects, security 1-1, 2-1–2-3
 - auditing and logging 2-3
 - authentication 2-1
 - authorization 2-2
 - integrity 2-2
 - obligation (non-repudiation) 2-3
 - privacy 2-3
- Audit Info System (AIS) 2-3, 3-15
- auditing 2-3, 3-15–3-16
 - user group 4-3
- authentication 2-1, 3-2–3-4
- authority checks 2-2, 3-5
- authorization 2-2
- Authorization Infosystem 2-2, 3-7

C

- CA900 Technical System Security course 4-2
- Complementary Software Program 3-10
- consulting 4-2, 4-1–4-3
- customer services 4-1–4-3

D

- data protection 4-3
- digital envelopes 2-3, 3-11, 3-13
- digital signatures 2-2, 2-3, 3-11–3-14

E

- encryption 2-3, 3-9, 3-11
 - with Internet applications 3-19

F

- feedback 4-3
- firewalls 3-8, 3-18

G

- GSS-API V2 3-9
- guidelines
 - audit R/2 4-3
 - audit R/3 FI 4-3
 - audit R/3 MM 4-3
 - data protection 4-3

I

- integrity 2-2
- Internet applications, security of 3-17–3-19
- Internet Transaction Server (ITS) 3-17, 3-18, 3-19
 - consulting services 4-3
- ITS See Internet Transaction Server

L

- locking mechanism 2-2
- locks, user and session 2-1, 3-4
- logging 2-2, 2-3, 3-15–3-16

N

- network communications 3-8–3-10
 - with Internet applications 3-18
- non-repudiation 2-3
- NT domain concept (consulting services) 4-2
- NT LAN Manager Security Provider (NTLMSSP) 3-3

O

- obligation 2-3

P

- passwords 2-1, 3-2
- PKI See Public-Key Infrastructure
- privacy 2-3
- private key 3-12
- Profile Generator 2-2, 3-6
- public key 3-11
- public-key certificate 3-11
- Public-Key Infrastructure (PKI) 3-13
- public-key technology 3-11

R

- R/3 authorization concept 2-2, 2-3, 3-5–3-7
 - workshop on 4-2

S

- SAP Audit User Group 4-3
- SAP Security Library (SAPSECULIB) 3-11, 3-14
- SAP Technical Consulting Services 4-1–4-3
- SAP Technical Consulting Services 4-1, 4-2
- SAP* 3-2
- SAProuter 3-8–3-9
 - using SNC protection 3-10
 - with the ITS 3-18
- SAPSECULIB See SAP Security Library
- screen savers 3-4
- Secure Network Communications (SNC) 3-9–3-10
 - authentication 2-1
 - integrity protection 2-2, 3-9
 - privacy protection 2-3, 3-9
 - Single Sign-On 3-3, 3-9
 - smart cards 3-3, 3-9
 - with the ITS 3-19
 - with the SAProuter 3-10
- Secure Sockets Layer protocol (SSL) 3-19

Index

Secure Store and Forward (SSF)	3-11–3-14	SSF	See Secure Store and Forward
integrity protection	2-2	<i>T</i>	
non-repudiation	2-3	Trust Center	3-13
See also digital signatures or digital envelopes		<i>V</i>	
Security Audit Log	2-3, 3-16	viruses	2-2
Security Consulting Team	4-1, 4-2, 4-1–4-3	<i>W</i>	
security guide, company-specific	4-2	Web server	3-17, 3-19
security policy	1-1, 1-2, 2-1	WGate	3-17, 3-18, 3-19
as part of CA900	4-2		
Single Sign-On	2-1, 3-3, 3-9		
smart cards	2-1, 3-3, 3-9		
SNC	See Secure Network Communications		

