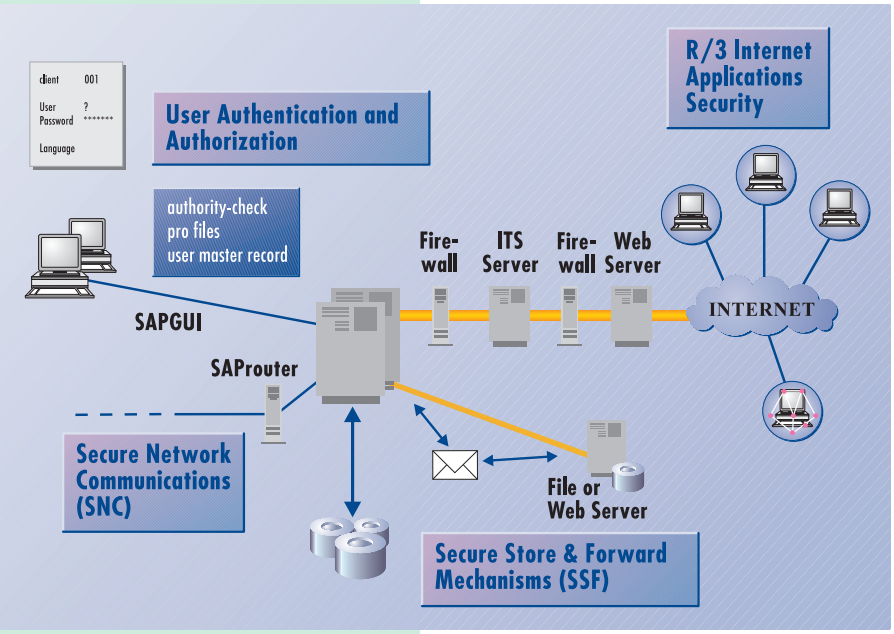
# R/3® System

# R/3 Security Mechanisms

The R/3 System offers a variety of security mechanisms to meet the demands on data protection, integrity, and confidentiality in today's business world. The most important features provided include:

- User Authentication and Authorization
- Auditing Tools
- R/3 Internet Applications Security
- Secure Network Communications (SNC)
- Secure Store and Forward Mechanisms (SSF)




## User Authentication and Authorization

At logon, users are authenticated through the use of passwords or smart cards. SAP® provides initial restrictions on passwords that you can expand upon to meet your own needs. Unsuccessful log-on attempts are retributed with session termination and user locks.

Once logged on, **authority checks** are performed to ensure that activities or transactions are only carried out by users who are authorized to do so. These authorizations are defined in Profiles and kept in the User Master Records. An initial set of profiles are predefined by SAP; you can modify and expand these profiles, or use the **Profile Generator** to automate the process of profile creation based on user activity information.

As of Release 3.1G, you can use the **Authorization Info System** to obtain an overview of your authorizations, profiles, users, and allocations.

## Auditing Tools

As of Release 4.0, you can use the **Audit Info System** to implement system-driven audits. This is a process-oriented reporting tool that displays all security-relevant information sources in the system in a clear and concentrated format. The **Security Audit** is also available to record security-related information and events in a productive system. By using these tools, you can quickly and easily identify gaps and risks in your authorization concept.

## R/3 Internet Applications Security

The design of the **SAP Internet Transaction Server** (ITS), provides for secure R/3 Internet Applications. The ITS Server acts as a stepping-stone between the Web Server and the R/3 Application Server. An Internet user requesting access to an R/3 System is first connected with the Web Server. A special SAP library installed on the Web Server communicates over a secure channel with the ITS Server. The ITS Server, located behind a firewall, does the direct communication with R/3.

## Secure Network Communications (SNC)

**Secure Network Communications (SNC)** provides protection for the communication links between the distributed components of an R/3 System. SNC enables you to use an external security product to increase the security level of your R/3 System. In addition to the standard security mechanisms offered by R/3, you can implement additional features offered by the external security product (for example: encrypted communications, Single Sign-On, or smart card authentication).

With SNC, the data exchanged between R/3 system components can be encrypted, providing for secure communications (for example, the confidential transfer of data between SAPgui and an R/3 Application Server).

With **Single Sign-On**, you only have to enter your password once, for the initial log-on to your security system or operating system. Your security system generates "credential" information for the user that is then used for automatic log-ons to further systems such as R/3. No password information is transmitted over the communication lines.

**Smart card authentication** allows for a safer authentication process. Because the user has possession of a card, which is also often protected with a password or PIN, it is much more difficult for someone to compromise a user's authentication information. Once again, no password information is transmitted over communication lines.

The most recent **SAProuter**, which is available with R/3 Release 4.0, also uses SNC features to establish secure communication tunnels between sites or other secured application areas. This is especially interesting if you have a R/3 release earlier than 3.1G, in which SNC is not available. By using an SNC-enabled SAProuter together with a firewall for communication outside your secured areas, you can communicate over secure channels between distant systems.

## Secure Store and Forward Mechanisms (SSF)

**Secure Store and Forward Mechanisms** provide the required support to protect R/3 data and documents as independent data units. By using SSF functions, you can "wrap" R/3 data and documents in secure formats, before they are saved on data carriers or transmitted over insecure communication links. A **digital signature** ensures that the data is not falsified and that the sender (signatory) can be clearly determined. The subsequently assigned **digital envelope** ensures that the contents of the data are only visible to the intended recipient(s). SSF also uses external security products.

As of Release 4.0, SSF can be used by various applications to protect data or to identify individuals. The following application areas use SSF as of Release 4.0 to implement digital signatures:

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

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.

## Future Plans

- Certification Process for External Security Products
- Central User Maintenance for distributed R/3 Systems
- Integration with Directory Services via LDAP
- Secure Authorization by an R/3 System for access over **ArchiveLINK® II**

Interested? Then call or write us.

## Technology and Service

The R/3 software is based on client/server architecture. It is designed as an open system that can be run on operating systems marketed by various vendors. However, SAP is not only a software provider: We also offer an extensive range of services and support centering around AcceleratedSAP (ASAP) – SAP's all-in-one solution for rapid implementation and ongoing optimization of R/3. The R/3 Service & Support program includes preventive system checks, data conversions, remote archiving and system upgrades. We provide expert organizational and technical consulting from the planning phase of your project right through to its execution, as well as in-depth training, and 24-hour support.

The quality management processes implemented for SAP development and SAP consulting in Germany comply with the international standard ISO 9001. SAP software is also the first packaged enterprise application software to receive "Ergonomics approved" certification for the international standards ISO 9241 and ISO 13407.



SAP Headquarters: SAP AG • P.O. Box 1461 • 69185 Walldorf • Germany • Tel.: +49.180.5343424 • Fax: +49.180.5343420
SAP International: Argentina: Buenos Aires • Australia: Sydney, Melbourne, Brisbane, Adelaide • Austria: Vienna, Linz, Salzburg • Belgium: Brussels • Brazil: Sao Paulo
Canada: Toronto, Calgary, Montreal, Ottawa, Vancouver • China: Beijing • Czech Republic: Prague • Denmark: Copenhagen • France: Paris • Hong Kong • Greece: Athens • Hungary: Budapest • Israel: Tel Aviv
Italy: Milan • Japan: Tokyo • Korea: Seoul • Malaysia: Kuala Lumpur • Mexico: Mexico City • The Netherlands: Hertogenbosch • New Zealand: Auckland, Wellington • Norway: Høvik • Philippines: Makati City
Poland: Warsaw • Portugal: Lisbon • Russia: Moscow • Saudi Arabia: Jeddah • Singapore • Slovakia: Bratislava • South Africa: Dunkeld West, Cape Town, Durban • Spain/Portugal: Madrid, Barcelona, Lisbon • Sweden: Stockholm
Switzerland: Biel, Lausanne • Thailand: Bangkok • Turkey: Istanbul • U.K.: Middlesex • United Arab Emirates: Dubai • USA: Wayne, PA; Philadelphia, PA; Boston, MA; Foster City, CA; Denver, CO;
Irvine, CA; Atlanta, GA; Irving, TX; Houston, TX; Chicago, IL; Minneapolis, MN; Cincinnati, OH; Cleveland, OH; St. Louis, MO; Parsippany, NJ; Pittsburgh, PA; Bellevue, WA