Secure Network Communications (SNC)

Secure Network Communications (SNC) provides protection for the data exchanged during communications between the distributed components of an R/3 System. In addition, SNC enables the use of cryptographic mechanisms and smartcards to securely authenticate users. This is accomplished by integrating an external security product with the R/3 System. The external security product can provide strong authentication, data integrity, and data confidentiality services for the R/3 System. The R/3 System administrator can adjust the level of protection desired (and possible with the external security product) using given R/3 System profile parameters for SNC.

When we refer to SNC, we are referring to a software layer that SAP has implemented within all relevant R/3 Basis components to achieve the protection goals described above. As the programming interface between the SNC layer and external security products we use the standardized *Generic Security Services Application Programming Interface (GSS-API) Version 2* [1;2]. This standard has been developed by the ”Common Authentication Technologies” (CAT) working group of the Internet Engineering Task Force (IETF)[1].

Several advantages for the customer offered by SNC are:

- Application level, end-to-end security is provided. This has certain benefits such as transport independence or transparent firewall traversal.[2]
- The use of **smartcards** for authentication is supported by certain products.
- Many network security systems implement **Single Sign-On,** so that a user’s initial authentication permits further automatic (re-)authentications of the user to distributed services. The ability to automatically (re-)authenticate is usually limited either to a period of time or by the presence of the smartcard in the reader.
- The transmission of passwords or passphrases over untrusted networks has been eliminated. With SNC, the R/3 System retrieves authentication information from the external security product without the need for R/3 password input by the end user.
- Each R/3 customer can use his favorite security product in compliance with national laws and this can be replaced at any time without affecting the application.

The frontend SAP Graphical User Interface (SAPgui) and the SAP Line Printer Daemon (SAPlpd) were the first components in Release 3.1 with the new security option to use other vendors’ network security products in conjunction with R/3. The provisions needed to link distant R/3 Systems and external programs securely via the SAP Remote Function Call (RFC) are available with Release 4.0.

[1] GSS-API Technical Information, RFC 2078 (working document)

[2] C-Bindings for GSS-API v2, RFC 2078 (working document)

[1] IETF is the standards body and open forum that defines and improves the protocols for the global Internet.
[2] The benefits obtained are dependent on the capabilities of the security product implemented.