Norwegian National Security Authority

Guide

Last updated: 2006-09-22
Version 1.01

SAP Security Guidance

Guide to the Security Act, Regulations concerning SAP Security

This document describes recommended technical security requirements for SAP systems within an information system classified BEGRENSET at System High mode of operation



Norwegian National Security Authority

The Norwegian National Security Authority (NSM) is a cross-sectoral professional and supervisory authority within the protective security services in Norway and administers Act of 20 March 1998 relating to Protective Security Services. The purpose of protective security is to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism. Protective security measures shall not be more intrusive than strictly necessary, and shall serve to promote a robust and safe society.

Purpose of guides

NSM's guidance activities are intended to build expertise and increase the security level of organisations through increased motivation, ability and willingness to carry out security measures. NSM regularly issues guides to help implement the requirements of the Security Act. NSM also publishes guides in other professional areas relating to protective security work.

Postal address
P.O. Box 14
1306 BÆRUM
POSTTERMINAL

Civilian phone/fax
+47 67 86 40 00/+47 67 86 40 09
E-mail address
post@nsm.stat.no

Military phone/fax
515 40 00/515 40 09

URL
www.nsm.stat.no

Table of Contents

1 Introduction 4
2 References 5
3 Abbreviations 6
4 Reading guidance 7
5 Security requirements 8
5.1 Integrated Security 8
5.2 Authentication 9
5.3 Authorization 10
5.4 Software distribution 13
5.5 Traceability / Audit 13
5.6 Availability 14
5.7 System management 15
5.8 Cryptographic mechanisms 16
5.9 Evaluated and Certified fundamental security functionality 16
Annex A Document History 17

1 Introduction

This guidance is targeted to SAP systems running on a platform classified at Norwegian level BEGRENSET, in a system high mode of operation. If SAP is to be used at a higher level of classification or in another mode of operation, the requirements may be subject to changes.

Focus of this guidance is on securing the SAP NetWeaver platform, more specifically the Web AS and the SAP clients. Which users should have access to different transactions and data, should be determined by the user's organization and the owners of the data. The level of access should be determined by the users' need to know in order to be able to do their job.

Suggestions and corrections are appreciated. Please provide your comments to post@nsm.stat.no, and type "SAP Security Guidance – Teknisk IT" in the subject field.

2 References

[1] ..... Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven / The Security Act) http://www.lovdata.no/all/nl-19980320-010.html

[2] ..... Forskrift om informasjonssikkerhet http://www.lovdata.no/for/sf/sf-19980320-010.html

[3] ..... NSM's guidance – V-FN-01 – Veiledning i grunnleggende sikkerhetsarkitektur og -funksjonalitet for FELLESNIVÅ operasjonsmåte www.nsm.stat.no (Regelverk, Veiledninger)

[4] ..... NSM's technological guidance – T-02 – Digital Certificates and Public Key Infrastructure in System High CIS www.nsm.stat.no (Regelverk, Veiledninger)

[5] ..... NSM's Standard cryptographic requirements, www.nsm.stat.no (Regelverk, Veiledninger)

[6] ..... Key words for use in RFCs to Indicate Requirement Levels http://www.ietf.org/rfc/rfc2119.txt

3 Abbreviations

ABAP	(SAP) Advanced Business Application Programming
AD	(Microsoft) Active Directory
AIS	(SAP) Audit Information System
CAPP	(CC) Controlled Access Protection Profile
CC	Common Criteria
CIS	Communication Information System
CUA	(SAP) Central User Administration
DoS	Denial of Service
EAL	(CC) Evaluated Assurance Level
EP	(SAP) Enterprise Portal
ERP	Enterprise Resource Planning
IETF	Internet Engineering Task Force
ITS	(SAP) Internet Transaction Server
J2EE	(Sun) Java 2 Enterprise Edition
LDAP	Lightweight Directory Access Protocol
NSM	Norwegian National Security Authority
RFC	Request for comments
SNC	(SAP) Secure Network Communications
SSO	Single Sign-On
Web AS	(SAP) Web Application Server
MS	Microsoft

4 Reading guidance

Requirements, prohibitions and warnings are placed in boxes in the following style. When there is more than one requirement in one section, the requirements are numbered.

Requirement paragraph style

Prohibition paragraph style

The Warning paragraph style

The words *Must/Shall* and *Should* are used according to IETF RFC 2119 [6].

MUST – This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

SHOULD – This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

5 Security requirements

The requirements defined in [3], [4] and [5] shall be met.

This document is an addition to [3] for SAP systems.

5.1 Integrated Security

1. SAP shall reuse the fundamental security functionality provided by the platform.

Existing security functionality should not be replaced or modified to fit specific applications. Neither should redundant security functionality be implemented if it is already available in the platform. A non-exhaustive list with examples of such functionality is application-specific logon, access controls, auditing and security management.

2. Third party SAP programs/tools should be certified by the SAP Software Partner program.

Certified programs that fully integrate with SAP are less likely to cause system instability and security breaches. Third party programs should reuse the security functionality available through SAP and the platform.

3. The system account running SAP should not have administrative privileges for all actions.

In the current version of SAP this requirement has to be violated in order to get support from SAP; however future versions of SAP should run as an unprivileged user for most actions. A more privileged system user could be used only for those actions where administrative privileges are necessary.

4. Invoking programs external to SAP on the SAP server shall not be allowed

External programs invoked through SAP on the application server, will run with the SAP system account's privileges, and not the invoking user's. Since the SAP account has administrative privileges, this may lead to escalation of user privileges. In future releases these programs must run within the invoking user's user context and privileges.

5.2 Authentication

Information systems must reuse the CIS' directory services for storage of system and security data.

Users should only have to log on once per session. SAP should be configured to use authentication mechanisms provided by the operating system for single sign-on. Requirements are defined in [3] chapter 5.1.3. Further authentication requirements are defined in [3] chapter 5.2.

5.2.1 Log-on

1. Authentication data must be protected.

Cryptographic mechanisms such as smartcard based two-factor authentication with PKI will be the preferred solution. A Kerberos based solution will also be acceptable. However the built-in Kerberos module in the operating system or any other critical component that handles the clear text password shall not be replaced. Replacing certified critical security components with application specific solutions will reduce trust and probably lead to interoperability problems with other software present in the information system.

2. The SAP proprietary logon mechanism is not acceptable.

SAP Logon does not utilize authentication mechanisms provided by the operating system, and transmits the user's password unencrypted over the network to the application server.

5.2.2 Directory service integration for authentication

SAP shall be integrated with the system's directory service.

SAP supports integration of the SAP user database, CUA, with a directory service. SAP utilizes the directory service for authentication and identity management.

A mapping between SAP user accounts and directory service user accounts has to be performed in SAP. The user accounts should have equal names in both user-databases, to ease the auditing process.

Failure of utilizing a directory service will result in a fragmented identity management and may result in users being assigned roles in different applications and systems that should not be combined.

5.3 Authorization

Applications must maintain and forward all relevant security attributes when caching or pooling resources on behalf of clients.

Pooling client connections to back-end servers is generally not recommended and may generate additional requirements for evaluation and certification.

SAP performs connection to the database as *one* shared DB-user for all activities of the SAP end-users. This design does not utilize the possibility of implementing user specific access control at the database level, based on the mechanisms provided by the database.

SAP authorizations are critical to security, as SAP omits the user based access controls in the database.

5.3.1 Authorizations / Access Control

1. Role / Authorization assignment shall be based on the principle of need-to-know.

Access controls in SAP are configured using *Authorizations*. Authorizations in SAP are positive, granting access; assignment of negative authorizations, denying access, is not possible. The effective authorizations of a user assigned with several roles, will be the aggregate authorizations of those roles. Due to the complexity of the authorizations necessary, roles should be based on SAP default roles with project specific extensions where necessary.

Role names ending with _ALL, _NEW or _ADM are critical. However keep in mind that all roles do not necessarily follow SAP naming conventions.

2. Authorizations should be revised on a regular basis.

Regular revision of authorizations should be performed to absorb changing needs for authorizations and to reveal too generous authorization assignments. When users are changing jobs or job roles, authorizations that are not necessary in the new job have to be removed.

3. No transaction, program nor report shall omit the authorization concept.

I.e. programs that do not have an *Authorization Group* and do not have AUTHORITY-CHECK statements inside the program shall not be allowed. The SAP platform should always enforce authorization checks.

5.3.1.1 Directory service integration for roles / authorizations

Authorization/role assignment should be done in an external directory service.

The SAP software requires that authorization information is stored in the CUA. Hence, authorization information should be synchronized from the directory service to SAP CUA.

5.3.1.2 Overview of the elements in the authorization concept

Authorization object: Groups 1 to 10 authorization fields together. These fields are checked simultaneously.

Authorization field: Smallest unit against which an authorization check should be run.

Authorization: An instance of an authorization object, a combination of allowed values for each authorization field of an authorization object.

Authorization profile: Contains instances (authorizations) for different authorization objects.

Role: Is a generated authorization profile. A role describes the activities of an SAP user.

Composite role: Consists of multiple roles. It cannot contain other composite roles.

User/User Master Record: Used for logging on to SAP systems and grants restricted access to functions and objects of the SAP system based on authorization profiles.

5.3.1.3 Authorizations assignment

Authorizations assignments should be made according to job roles. Each user and system account should only be assigned the minimum of authorizations needed to perform the job according to the principle of need-to-know. When a new user is created, it does not have any pre-assigned authorizations.

SAP_ALL grants practically unrestricted access to the entire system and shall not be granted.

SAP_NEW provides authorizations for new authorization objects, and leads to unwanted authorization enhancements. SAP_NEW shall not be granted.

5.3.1.4 Powerful transactions

Transactions that give direct access to the database or operating system must not be allowed.

If a user is granted direct access to the operating system or the database through SAP, due to the design of SAP, the user will perform those actions as the SAP system user with this user's privileges.

Some transactions allows the user to launch programs on the server OS or directly manipulate the database tables.

Examples of powerful transactions are SA38/SE38, where users may start reports. These transactions are at risk in combination with reports without authorization checks.

5.3.2 Users

1. All interactive user accounts shall be personal.

Activities of users with extensive authorizations assigned and non-personal user accounts should be monitored extra carefully.

If non-personal user accounts are necessary, a log of who is logging on with the user account has to be maintained.

2. All default passwords must be changed and conform to the password rules in [3], even if accounts are disabled.

5.3.2.1 SAP*

Remove all authorizations from the default user SAP*. Add SAP* to the SUPER user group in all clients, to ensure that only authorized administrators can change its user master record. If deleted, the user will still be available with a hard coded default password. SAP* should never be unlocked.

Disable the hard-coded SAP* user with the following parameter:

Login/no_automatic_user_sap* =1

Do not delete the user SAP*! *SAP* is hard-coded in SAP Systems and does not require a user master record! If a user master record for SAP* does not exist in a client, then anybody can log on to the SAP System as the user SAP* using the well-known password PASS. In this case, SAP* is not susceptible to authority checks and has all authorizations. Therefore,* ***do not delete SAP**** *from any client.*

5.3.2.2 DDIC

DDIC should not be assigned the SAP_ALL profile. DDIC should always be locked. Unlock it only when necessary. Use of DDIC should be limited to a minimum and personal accounts for administration should be used as widely as possible.

5.3.2.3 EarlyWatch

EarlyWatch shall not be performed from outside the classified platform.

EarlyWatch should always be locked.

5.3.2.4 SAPCPIC

SAPCPIC is an older user, should be locked where present.

5.4 Software distribution

Software and patches shall be integrity protected.

Software and patches shall be received from the vendor in a secure fashion. If cryptographic mechanisms are used, these cryptographic mechanisms must be approved by NSM.

5.5 Traceability / Audit

Auditable events are defined in [3] 5.6.2, points a through h.

1. All audited events shall be traceable back to an individual person.

All actions of a person should be performed with the same identity throughout the system, i.e. the same identity to access the operating system, the database and SAP. Audit information should contain information about the user trigging the auditable event, wherever the event occurs.

2. Audit data shall be centrally stored.

Audit data generated locally must be consolidated to a central log server. The central log servers should have tools for analyzing and acting on events. Tools should be designed to discover patterns of attempted or successful misuse. Critical events should trigger alerts sent to administrators.

3. Administrators must not be able to modify log data. Audit and administrator roles should be separated.

The role as the system security auditor should not be given to persons responsible for administration of the system. Administrators are the most privileged users in the system, and should be subject to auditing themselves. The users used for auditing purposes should have minimal privileges besides access to audit information. Of course administrators are also allowed to access the audit logs, in order to be able to do their jobs.

4. Purging of the audit logs should be audited.

Purging the audit logs may be done to cover the tracks of unauthorized actions. This event should be audited **after** the purging has been performed.

5.5.1 Audit Information System

SAP Audit Information System (AIS) is the SAP auditing tool for system and business audit. Business audit is not within the scope of this guidance.

AIS is used to configure auditable events and provides audit reports based on given criteria. Access to AIS is regulated based on roles and authorizations.

System audit is divided into three main areas:

- general system
- users and authorizations
- repository and tables

The security audit log is recorded in an audit file on each application server. These files must be consolidated to a central log management tool.

Development of available log space shall be monitored.

When the maximum audit file size is reached, the auditing process stops. The maximum size of the log files must be set in relation with the log consolidation interval and the amount of audit data recorded under intensive system usage. SAP systems maintain audit logs by days, but SAP does not automatically overwrite old log files from previous days. These have to be archived and deleted.

Audit logs must be archived according to NSM regulations in [3], section 5.6.7. Original log files may be deleted when archiving is performed. SAP prevents purging of audited events less than three days old. In the Security Audit Log *Reorganization* tool, the default *minimum age* of log files to delete is 30. Backed up logs may be deleted from the production system when they're no longer necessary for management purposes.

5.6 Availability

1. A high availability of the system must be ensured.

The system should resist accidental failure and targeted attacks on availability.

2. System activity and performance level of the system should be monitored.

5.6.1 Redundancy

By implementing autonomous redundant systems on different physical locations vulnerability of accidental downtime is reduced.

5.6.2 Backup

Backup should be done regularly and automatically

Both system configuration and system data should be backed up.

Re-do logs for the database should be kept separate from the database, on designated disks, and backed up.

5.6.3 Resistance to Denial of Service attacks

The system shall not be configured in such a way that it's vulnerable to DoS attacks.

Examples of such configuration are:

- To lock out user accounts for a long time after consecutive unsuccessful logon attempts. As mentioned in [3] section 5.2.8 the account lockout policy should be considered carefully not to conflict with availability.
- Allowing full log files to stop the system.
- Too little disk space available for log files compared to the level of auditable events.
- Filling the audit log with events that could quickly be generated by an attacker.

5.6.4 Resource controls

Users should not be allowed to start processes that consume all available resources

5.7 System management

System management should be done through a shared tool for all applications running on the platform, providing an integrated overview of the entire system.

All management tasks should be provided and done from this management tool. SAP supports management through third party tools like MS Operations Manager and HP OpenView.

System management and support shall not be performed through connections to other nations.

Support through VPN connections to Walldorf is not acceptable.

5.8 Cryptographic mechanisms

By [1] §14, only cryptosystems that have been approved by NSM are allowed to be used to protect sensitive information.

Examples of cryptographic usage are authentication mechanisms, integrity protection of software, confidentiality protection of administrator traffic and other sensitive information.

5.9 Evaluated and Certified fundamental security functionality

1. Fundamental security functionality shall be evaluated and certified.

The preferred solution is to reuse already certified solutions provided within the system infrastructure. The evaluated and certified components must be utilized with the designated approach.

2. Security functionality shall be evaluated and certified according to CAPP, or a similar set of requirements, at level EAL 3 or higher.

For dedicated and system high systems at BEGRENSET, EAL 3 will be sufficient. For systems at higher classification levels, as well as system high mode security functionality in partitioned systems, EAL 4 shall be chosen.

5.9.1 Certification status

SAP is not certified according to the CC standard.

SAP's proprietary security functionality circumvents built-in security functionality in both OS and DB.

In order to comply with requirement 2 in the previous section, either SAP's security functionality must be evaluated and certified, or already evaluated components must be reused. The latter is the preferred solution. For some security functionality this is possible today. These options should be utilized.

Annex A Document History

2005-08-15	Document created.
2006-09-22	Layout changes only.