SAP NetWeaver 2004s SPS 4

Security Guide

Security Guide for SAP NetWeaver BI

Document Version 1.00 – October 24, 2005

THE BEST-RUN BUSINESSES RUN SAP

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this documentation at the following Internet address:
`service.sap.com/securityguide`

THE BEST-RUN BUSINESSES RUN SAP

SAP®

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, *F2* or *ENTER*.

Icons

Icon	Meaning
⚠	Caution
💬	Example
💡	Note
🧭	Recommendation
SYN	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

Security Guide for SAP NetWeaver BI

⚠

This guide does not replace the handbook for daily operations that the customer is supposed to create for productive operation.

About this Guide

This guide describes the security-relevant aspects of the usage types BI and BI Java, which are based on the usage types AS ABAP and AS Java. As such, the guide describes the security information that is different or additional to the usage types AS ABAP and AS Java.

The usage type BI and BI Java support the scenarios Enterprise Data Warehousing, Enterprise Reporting, Query, and Analysis, as well as Business Planning and Analytical Services. If you want to implement these scenarios, additional usage types are required.

The following table provides an overview of the relevant security guides:

Application	Security Guide
Application Server for ABAP Application Server for Java	SAP NetWeaver Application Server ABAP Security Guide [SAP Library] SAP NetWeaver Application Server Java Security Guide [SAP Library]
Enterprise Portal Knowledge Management	Portal Security Guide [SAP Library] Knowledge Management Security Guide [SAP Library]
Process Integration	SAP NetWeaver Process Integration Security Guide [SAP Library]

Why Is Security Necessary?

SAP NetWeaver BI serves to integrate, transform, and consolidate data from all areas of an enterprise in order to provide this for analysis, interpretation and distribution. This includes confidential corporate data, for example, personal data from Personnel Administration. Decisions are made in all enterprise areas and target-oriented actions are determined on the basis of this data. For this reason, security when accessing data and the ability to guarantee data integrity is of great importance.

The following examples show the dangers to which BI can be exposed:

- Attacks from the Internet or Intranet when using BEx Web functionality and Web Services
- Infringement of data protection guidelines through unauthorized access to personal data

Target Groups

- Technical consultants
- System administration

1 User Administration and Authentication

1.1 User Management

BI uses the user management function that is delivered for the ABAP and Java SAP NetWeaver Application Platforms.

See also:

User Management [SAP Library]

Users

Standard users created when the BI system is installed

See Protecting Standard Users [SAP Library]

⚠

Change initial passwords after installation to ensure that standard users cannot be misused.

Standard users specified when the SAP J2EE Engine is installed

See *SAP NetWeaver Application Server Java Security Guide* → *User Administration and Authentication* → *User Administration and Standard Users* → *Standard Users* and → *Standard User Groups.*

⚠

Change initial passwords after installation to ensure that standard users cannot be misused.

Users in BI and SAP Source System

The following table provides an overview of additional users required when using the BI and BI Java usage types: These users are not delivered and do not have default passwords.

System	Users	Type	Description
BI	Database user		For more information on database users, see Operating System and Database Platform Security Guides [SAP Library]
BI	Background user in BI (**BWREMOTE**)	Technical user	The background user in BI is used for communication with the BI source systems, for the extraction of data, and for background processes in BI. You create the background user in BI in the Implementation Guide and assign it a password (*SAP NetWeaver → Business Intelligence → Automated Processes → Create User for Background Processes*). SAP recommends that you call the BI background user **BWREMOTE**. The system asks for a background user password when connecting to the source system. The authorization profile for the background user is S_BI-WHM_RFC. **See also:** Authorization Profile for Background Users [SAP Library].
SAP source system	Background user in SAP source system (**ALEREMOTE**)	Technical user	The background user in the SAP source system is used for communication with BI and for the extraction of data. If you connect an SAP source system to BI, the background user is to be created in the source system. You can create the user directly in the source system in user maintenance. You can enter a name in the Implementation Guide in BI that will be used as the default name for the background user when you connect a new source system. (See *SAP NetWeaver → Business Intelligence → Links to Other Systems → Connections Between SAP Systems and BI System → Maintain proposal for users in the source system (ALE communication).* SAP recommends that you call the BW background user for the source system **ALEREMOTE**. If the source system you are using is also a BI system, SAP recommends that you create the background user for BI and the background user for the (BI) source system completely separately. The authorization profile for the background user in the source system is S_BI-WX_RFC. **See also:** Authorization Profile for Background Users [SAP Library].

System	Users	Type	Description
BI	Administrator	Individual user	The BI administrator is responsible for the connection to source systems, loading of metadata and implementation of BI statistics, among other things. This user develops the data model and plans and monitors the processes in BI (such as the loading process). **See also:** Authorization Profile for Working with the AWB [SAP Library]
BI	Authors and analysts	Individual user	Authors and analysts require advanced analysis functionality and the ability to examine ad-hoc data. In order to accomplish their tasks, they required useful, manageable reporting an analysis tools. **See also:** Authorizations for Query Definition and Information Broadcasting [SAP Library]
BI	Executives and Knowledge Workers	Individual user	Executives and Knowledge Workers require personalized, context-related information that is accessible via an intuitive user interface. They generally work with pre-defined navigation paths, but require the option of analyzing the summary data more deeply. **See also:** Analysis Authorizations [SAP Library]
BI	Information Consumers	Individual user	Information Consumers require specific information (snapshot of a specific data set) in order to be able to execute their operative tasks. **See also:** Analysis Authorizations [SAP Library]

1.2 Authentication and Single Sign-On

The authentication process enables the identity of a user to be checked before this user gains access to BI or BI data. SAP NetWeaver supports various authentication mechanisms.

See also:

User Authentication and Single Sign-On [SAP Library]

Integration in Single Sign-On Environments

User ID and Password

BI uses a user ID and a password for logon (see Logon and Password Security in SAP Systems [SAP Library]).

Secure Network Communications (SNC)

BI supports Secure Network Communications (SNC) [SAP Library].

SAP Logon Tickets

BI supports SAP logon tickets. To make Single Sign-On available for several systems, users can issue an SAP logon ticket after they have logged on to the SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.

For more information, see SAP-Logon Tickets [SAP Library]

Client Certificates

As an alternative to user authentication using a user ID and passwords, users using Internet applications via the Internet Transaction Server (ITS) can also provide X.509 client certificates. In this case, user authentication is performed on the Web Server using the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

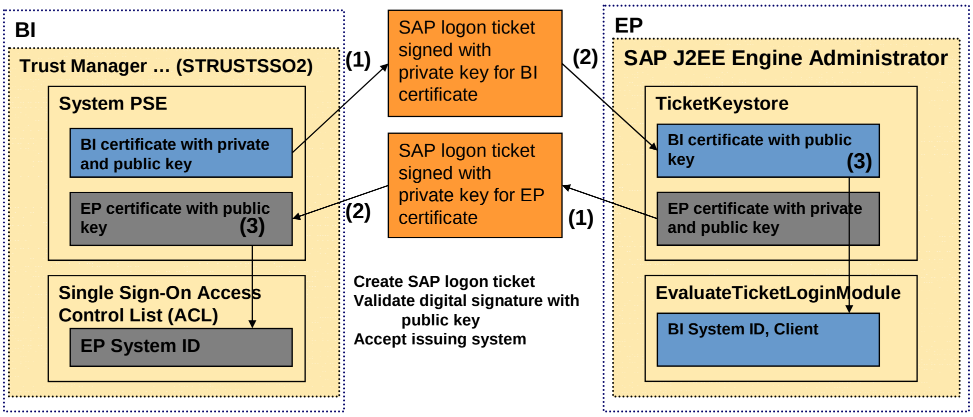
You can find more information under X.509 Client Certificates [SAP Library].

Integration into the SAP NetWeaver Single Sign-On Environment

The Enterprise Portal (EP) is the central entry point for the user within SAP NetWeaver. EP supports and issues SAP logon tickets. BEx Web Applications are usually called from the Enterprise Portal. The close integration of BI and EP enables access from BI as well, where Single Sign-On is also supported.

The following graphic illustrates the interaction between BI and EP in terms of single sign-on:

- **BI trusts SAP logon tickets from EP because the public key of the EP certificate has been imported into BI**
- **EP trusts SAP logon tickets from BI because the public key of the BI certificate has been imported into EP**


BI
Trust Manager … (STRUSTSSO2)
System PSE
BI certificate with private and public key
EP certificate with public key
(3)
Single Sign-On Access Control List (ACL)
EP System ID
(1)
(2)
SAP logon ticket signed with private key for BI certificate
SAP logon ticket signed with private key for EP certificate
(2)
(1)
Create SAP logon ticket
Validate digital signature with public key
Accept issuing system
EP
SAP J2EE Engine Administrator
TicketKeystore
BI certificate with public key
(3)
EP certificate with private and public key
EvaluateTicketLoginModule
BI System ID, Client

1.2.1 Authentication: Enterprise Reporting, Query, and Analysis

In the Enterprise Reporting, Query, and Analysis scenario, users have to be authenticated in a Single Sign-On environment when performing the following tasks:

Calling BEx Web Applications from the Enterprise Portal [Page 11]

Information Broadcasting in the Web [Page 12]

Information Broadcasting as Background Processing [Page 11]

Publishing to the Enterprise Portal [Page 13]

Calling BEx Web Applications from the Enterprise Portal

Calling BEx Web Applications from the portal corresponds to calling applications from other components. Single-sign on means that you do not have to log on to BI manually.

Overview

Portal (explicit authentication at the portal; Web browser receives portal ticket)	→	BEx Web Application (implicit authentication at BI with portal ticket)

For single-sign on when calling BEx Web Applications from the portal, the following settings have to be made in the Implementation Guide at *SAP NetWeaver* → *Business Intelligence* → *Reporting-Relevant Settins* → *BEx Web* → *Integration into the Enterprise Portal*.

- BI system must accept tickets (maintain single sign-on in BI system)
- BI system must have imported portal certificates in order to authenticate tickets from the portal (export portal certificates; import portal certificate)

Information Broadcasting as Background Processing

During precalculation and distribution of BW reports using background processing, BEx Web applications are executed and the generated HTML documents are stored in the Knowledge Management folder or distributed by e-mail.

Broadcast settings are executed in the background,

- if they were registered for execution at a specific time
- if they were registered for execution upon data change and the event *Data Change* was triggered by a process chain
- if they were scheduled directly in background processing

This is how a scheduling user who has performed registration or scheduling executes broadcasting settings for another user.

This is the case

- when the authorization user in the broadcast settings is not the scheduling user
- if the broadcast setting requires a user-specific execution for people other than the scheduling user

For security reasons, when processing in the background, the system checks whether the scheduling user is authorized to schedule background tasks for one or more users (authorization object S_BTCH_NAM).

A job can be executed in the background under various user names so that the HTML documents are generated according to user-specific authorizations.

Storage in a Knowledge Management folder takes place through an RFC call from ABAP to Java. A general Portal Service User (bw_service) is used on the Java page. This Portal Service User must have write authorization for the appropriate Knowledge Management folder.

The documents stored in Knowledge Management receive the Portal Service *User* as value in the attribute *Generator*. This enables easy differentiation between documents that were created by one user or those that were created during background processing.

When using distribution by e-mail and precalculation of BW workbooks using MS Excel, functions from the portal are not required.

Overview

Precalculation and generation of documents (explicit authentication in the BW occurs during job scheduling)	→	Storage of documents in Knowledge Management (implicit authentication at the portal as Portal Service User bw_service)

You can find additional information on precalculation under Functions of the BEx Broadcaster [SAP Library].

Information Broadcasting in the Web

Direct distribution or setting of scheduling for background processing of BEx Web applications can be done in the Web using the BEx Broadcaster.

The BEx Broadcaster is a special BI Web item that behaves like a normal BEx Web Application and runs within BI. There is input help for selecting a Knowledge Management folder for storing the precalculated documents. This is realized as a portal iView (com.sap.ip.bi.portalnavigation.folderselection).

Three different scenarios can be classified:

1. If the BEx Broadcaster is called directly in the Web browser, an authentication at the BI system needs to take place. When calling the input help for the KM folder, a second authentication with the portal needs to take place.

Overview

BEx Broadcaster (explicit authentication at BI, Web browser receives BI ticket)	→	Input help (explicit authentication at the portal because the portal does not accept a BI ticket)

2. If the BEx Broadcaster is called from within the portal, authentication takes place implicitly with the BI system if the appropriate single sign-on has been set up between the portal and BW (see Calling BEx Web Applications from the Portal [Page 11]).

Overview

Portal (explicit authentication at the portal; Web browser receives portal ticket)	→	BEx Broadcaster (implicit authentication at BI with portal ticket)	→	Input help (implicit authentication at the portal with portal ticket)

3. If the settings described in the following, under Publishing to the Enterprise Portal [Page 13] have been made, the portal also accepts tickets from the BI System. Then the explicit authentication at the portal (described under point 1) that occurs when calling the input help does not apply.

Overview

BEx Broadcaster (explicit authentication at BI, Web browser receives BI ticket)	→	Input help (implicit authentication at the portal because the portal does not accept a BI ticket)

Multiple portals can be connected to a BI system (see SAP NetWeaver → *Business Intelligence* → *Reporting-Relevant Settings* → *BEx Web* → *Integration into the Enterprise Portal* → *Maintaining Portal-Server Settings for EP*)in the implementation guide. The portal that is designated as the standard portal is used when the input help for the KM folder is called.

Publishing to the Enterprise Portal

When publishing in the Enterprise Portal in the BEx Web Application Designer, the portal roles assigned to the user and the personal folders in Knowledge Management are displayed.

To get this personalized information from the portal in the BEx Web Application Designer, the user in the BW system has to be assigned a user in the portal. Assignment is not necessary if the technical user name in SAP EP and in SAP BW are identical. After assignment, authentication of the portal user must be made. Authentication takes place using the BW ticket that the BEx Web Application Designer receives during explicit logon. The portal requires the BW certificate to validate the BW tickets.

Overview

BEx Web Application Designer (explicit authentication at BW, BW ticket available)	→	Portal (implicit authentication at the portal with BW ticket)

For publishing to the portal in the BEx Web Application Designer, the following settings have to be made in the Implementation Guide at *SAP NetWeaver* → *Business Intelligence* → *Reporting-Relevant Settins* → *BEx Web* → *Integration into the Enterprise Portal*:

- The BW system must generate tickets (maintain single sign-on in BI system)
- The portal must have imported the BW certificate in order to authenticate tickets from SAP BW (export BI certificate; import BI certificate).
- You must maintain user assignments in the portal if the technical user names are different from one another (maintain user assignment in EP).

2 Authorizations

To ensure that the Data Warehousing solution represents the structure of your company and fulfills its requirements, you have to define who has access to which data.

An authorization allows a user to perform a certain activity on a certain object in the BI System. There are two different concepts for this depending on the role and tasks of the user: standard authorizations and analysis authorizations.

An authorization concept must always have already been taken into account in the modeling phase. Otherwise there could be functional or security restrictions.

Standard Authorizations

These authorizations are required by all users that are working in the Data Warehousing Workbench to model or load data, and also by users that work in the planning workbench or the Analysis Process Designer and those that work with the Reporting Agent or the BEx Broadcaster or define queries.

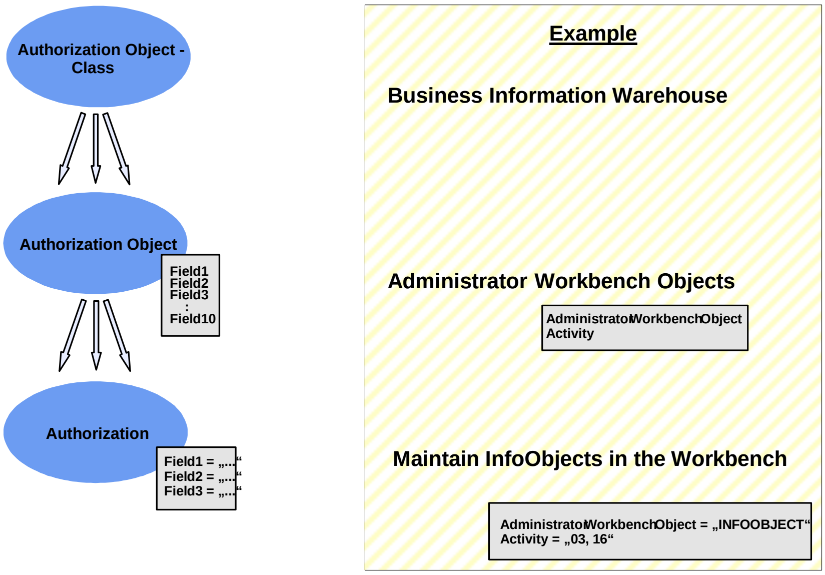
Each authorization refers to an authorization object and defines one or more values for each field that is contained in the authorization object. Individual authorizations are combined into roles by system administration. You can copy the roles delivered by SAP and adjust them as needed. The system administrator creates these authorizations and enters them into individual users' master records in the form of profiles.

For more information, see Standard Authorizations [SAP Library].

These authorizations are based on the **standard authorization concept of SAP**.

For more detailed documentation on the SAP authorization concept, see SAP Authorization Concept [SAP Library].

Structure of Authorizations


Authorization Object - Class
Authorization Object
Field1
Field2
Field3
:
Field10
Authorization
Field1 = „...“
Field2 = „...“
Field3 = „...“
Example
Business Information Warehouse
Administrator Workbench Objects
AdministratorWorkbenchObject
Activity
Maintain InfoObjects in the Workbench
AdministratorWorkbenchObject = „INFOOBJECT“
Activity = „03, 16“

Analysis Authorizations

All users that want to display transaction data from authorization-relevant characteristics in a query require analysis authorizations for these characteristics.

This type of authorization is **not** based on the standard authorization concept of SAP. Instead, they use their own concept that takes the features of reporting and analysis in BI into consideration. More and more users are gaining access to query data with the distribution of queries using the BEx Broadcaster and publication of queries to the portal. With the special authorization concept of BI for the display of query data, you can protect especially critical data in a much better way.

For more information, see Analysis Authorizations [SAP Library].

Previous to SAP NetWeaver 2004s, the SAP standard authorization concept was also used for analysis authorizations, then called reporting authorizations. If you have upgraded to SAP NetWeaver 2004s, you can decide whether you want to use the new, more user-friendly concept or switch back to the previous reporting authorization concept. If you decide to use the new concept, the old reporting authorization objects will no longer be taken into account (access is denied).. However, SAP recommends using the new concept because it is better suited to the requirements of BI and because the previous concept will no longer be supported.

For more information about the previous concept of reporting authorizations, see Previous Concept for Reporting Authorizations [SAP Library].

Types of Functions of Authorizations

With authorization checks, any functions, objects or values in the system can be protected. With an authorization check, when you perform a certain action, the system compares the values for the individual fields of an authorization object or an authorization that are assigned to the user with the values that are provided for the execution of an action in the program. A user is only authorized to perform an action if the authorization check has been successful for **every field** in an authorization object or in an authorization. In this way, complex checks of the user authorization can be carried out.

2.1 Authorization Log for Analysis Authorizations

A tool is available in the analysis authorizations to analyze authorization checks. It provides detailed information on the authorization-relevant data access instances. This check can be switched on or off on either a permanent basis or as and when required, depending on the users involved. Access to this analysis tool is to be protected using the transaction RSECPROT and the authorization object S_RSEC. Only authorized users are to have access to the tool.

See also:

Error Log [SAP Library]

2.2 Checking Analysis Authorizations as Another User

In the administration for analysis authorizations you can execute certain transactions as another user by choosing the function *Execute as...* on the *Analysis* tab page. All the checks for analysis authorizations (only) are then run for the defined user. It is possible, therefore, that a user could gain access to more authorizations than he or she would normally have. For this reason, this transaction should be protected using the authorization object S_RSEC.

See also:

Management of Analysis Authorizations [SAP Library]

Overview: Authorization Objects [SAP Library]

3 Communication Security

3.1 Communication Channel Security

The following table provides an overview of the communication channels and the technology used in each case:

Communication between…	Technology used for communication	How is data protected?
Front end and application server	RFC	See RFC / ICF Security Guide [SAP Library]
Application server and application server	RFC	See RFC / ICF Security Guide [SAP Library]
SAP J2EE Engine and application server	RFC	See RFC / ICF Security Guide [SAP Library]
SAP router and application server	RFC	See RFC / ICF Security Guide [SAP Library]
Connection to database	RFC	See RFC / ICF Security Guide [SAP Library]
Web Browser and application server	HTTP, HTTPS, SOAP	

When using Web applications, we recommend that you switch on encryption for HTTPS.

3.2 Communication Destinations

Connection destinations are required in BI in the following areas:

- BEx Web

  RFC destinations in the J2EE Engine

  RFC destination for the portal

  For more information, see the Implementation Guide (IMG) for SAP NetWeaver and choose *Business Intelligence* → *Reporting-relevant Settings* → *BEx Web* → *Integration into SAP Enterprise Portal 6.0*

- Use of TREX

  RFC destination in the BI system

  See the Implementation Guide for SAP NetWeaver → *Business Intelligence* → *Connectivity of TREX*

- Connection of data sources to BI system

  These destinations are usually not delivered but are created by customers.

If you want to connect SAP systems and non-SAP data sources as source systems to BI, you usually need RFC destinations.

To use UD Connect you need an RFC destination for the J2EE Engine. Communication between the J2EE Engine and the BI server is undertaken by the JCo. See the Implementation Guide for SAP NetWeaver → *Business Intelligence* → *UDI Settings by Purpose* → *UD Connect Settings*.

The destination for a Myself BI is created automatically by the system the first time you open the BI Data Warehousing Workbench.

XML data is sent to the SAP Web AS SOAP service using specific ports, then into BI. For more information, see Sending Data to the SOAP Service [SAP Library].

The communication between BI and source systems is the responsibility of BI background users and the background users in the source system (in the case of the SAP source systems). The BI background user requires the authorization profile S_BI-WHM_RFC. The background user in the SAP source system requires the authorization profile S_BI-BW_RFC. For more information, see Authorization Profiles for Background Users [SAP Library].

4 Security with Data Storage

In BI, data is stored on the SAP Web application server database.

If an end-user is evaluating data using Microsoft EXCEL, s/he can also store her/his data locally. The end-user has to make sure that no unauthorized person can access the locally stored data.

If BI evaluations and analysis are called using BEx Web applications, data is displayed in a Web Browser. Data is then stored in a browser cache. SAP recommends that you always delete the browser cache when you have evaluated the data.

BEx Web applications can be implemented either as applications with a state or without a state. Use the BI Web runtime for Web application session cookies with a state to combine independent requests (that is, the function calls in a Web application, for example, navigation steps) for a session. Such cookies are called sap-contextid. The cookie contains a generated ID as a value. This ID allows the relevant session to be identified by the server. The session cookie is a temporary cookie and is deleted automatically when the browser window is closed. The server also has a timeout parameter. The session cookie is invalid after the timeout and can no longer be used for navigating in a Web application. You can use the session coding in the URL for the Web application by using the Web template attribute **NO-SESSION_COOKIE**. In this case, no session cookie is generated. So that the Web application uses the session coding in the URL, set **X** for the attribute **NO-SESSION_COOKIE**. Also see Object Tag for the Properties of Web Templates [SAP Library].

You can protect data from being accessed by an unauthorized end-user by assigning analysis authorizations. Data is not protected by the default settings. However, you can flag InfoObjects in BI as being authorization-relevant (see also: Tab Page: Business Explorer [SAP Library]). Then data can only be accessed if the user has the required authorizations.

Data in BI is predominantly accessed for read purposes. However, in Business Planning and Simulation [SAP Library] data is also changed.

5 Minimal Installation

BI uses JavaScript in the Web Browser when executing Web Applications. You can deactivate JavaScript for a minimal configuration. However, we recommend that you do **not** deactivate JavaScript. Deactivating JavaScript means that it is no longer possible to use all of the Web items and dialogs in the Web without restrictions, and the navigation options in Web applications are considerably limited.

6 More Information Relevant to Security

Using Active Code

BI uses JavaScript on the client machine in the Web browser when executing Web applications.

See Minimal Installation [Page 18]

Encryption of E-Mails When Distributing Business Intelligence Content

Information Broadcasting uses the SAP NetWeaver interface SAPconnect to create and send e-mails with Business Intelligence content. This interface does not support encryption or certificates. Therefore, e-mails that are created in the SAP system using Information Broadcasting are not encrypted or provided with certificates.

However, SAP provides an additional product from another provider (the Secure Email Proxy) so that you can encrypt e-mails.

See SAPconnect [SAP Library], and in particular, the section Secure Email [SAP Library]