PUBLIC

SAP Cloud Handbook

Document Version: 1611 - 2016-11-10

SAP Business ByDesign

Security Guide

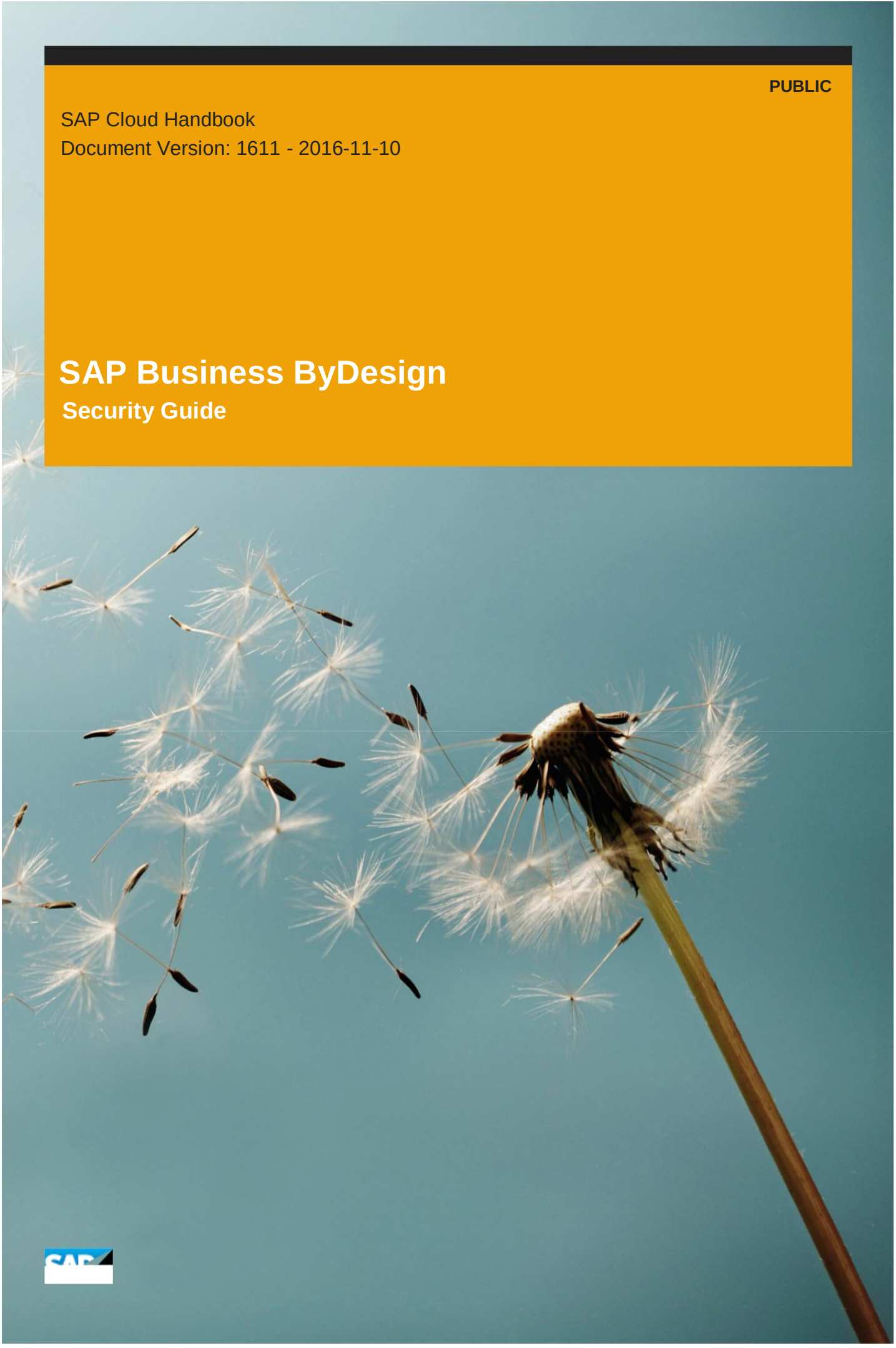


Table of Contents

1 Document History

Version	Date	Change
1.0	2013-11-20	Initial version for SAP Business ByDesign, SAP Cloud for Customer and SAP Cloud for Travel and Expense November 2013
1.1	2013-11-28	The following chapters have been updated: • Business-to-Business Communication and Application Integration • Logon Using Client Certificate (X.509)
1.2	2014-09-05	Miscellaneous typographical errors corrected. No technical updates made to the content
1.3	2016-11-06	Removed references for other cloud products and SSL protocol

2 Introduction

2.1 About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Business ByDesign,

2.2 Why is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, demands on security are also on the rise.

When using a distributed system, you must ensure that your business processes do not permit unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These security requirements apply equally to SAP Cloud solutions.

To assist you in ensuring the security of your SAP Cloud solution, we provide this Security Guide.

2.3 Document Structure

The Security Guide contains the following sections:

- Technical System Landscape
  This section describes the technical components and communication paths that are used in the solutions.
- User Administration and Authentication
  This section describes the user administration tools, and the system access and authentication concept that applies to the solutions.
- Authorizations
  This section describes the authorization concept of the solution.
- Mobile Applications
  This section describes mobile applications.
- Front-End Security
  This section describes the security mechanisms that apply to the front end.
- Security of Data Storage and Data Centers
  This section describes critical data that is used by the solutions, and the security mechanisms that apply.
- Security for Additional Applications
  This section contains security information about additional software components that are associated with the solutions.
- Other Security-Relevant Information
  This section contains information about service composition security, and internal and external audits.
- Security-Relevant Logging and Tracing
  This section describes trace and log files that contain security-relevant information, allowing you to reproduce activities if a security breach occurs.

3 Technical System Landscape

SAP Cloud solutions are hosted in SAP's own data center located either in Germany, the United States of America or Australia. Customers can choose in which data center their solution shall run.

The solutions provide optional integration with a full Enterprise Resource Planning (ERP) suite, including the associated server landscape and system maintenance.

Since SAP Cloud solutions deal with business data from your core business processes, SAP adheres to the highest security and quality requirements, as follows:

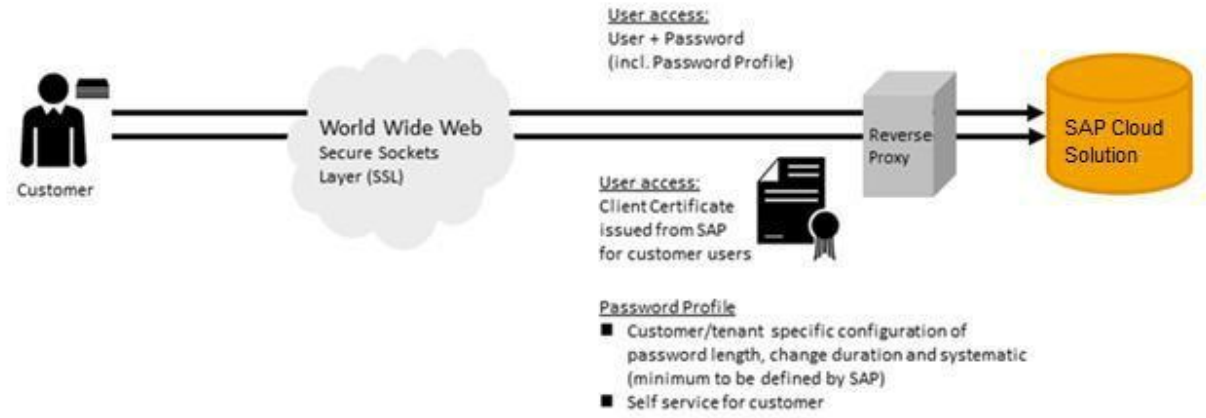
- The business data is stored securely in SAP data centers.
- Customers share physical hardware, but their data is separated into tenants.
- Users who require access to the business data must authenticate themselves, and their identity must be verified by user and access management.
- Customer data always belongs to the customer.

You can access your SAP Cloud solution in the following ways:

- Desktop computer: browser-based Internet access from any network with internet access
- Portable computers: browser-based Internet access from any network with internet access
- Mobile devices: Native Apps (SAP Cloud for Travel and Expense provides native apps. Access to SAP Cloud for Travel and Expense via a Web browser on a mobile phone or table is neither supported nor recommended.)

Industry best practices and state-of-the-art open cryptographic standards secure and protect communications between customer devices and the system landscapes of your SAP Cloud solution in the SAP data center.

The following diagram summarizes the technical system landscape for standard access:



To access SAP Cloud solutions, you must enter a unique, customer-specific URL.

Communication is carried out via the Reverse Proxy (RP) component in the SAP data center.

The Reverse Proxy is the SAP Web Dispatcher, which is developed and maintained by SAP Cloud Support.

The communication channels that require mutual authentication are secured by using standard Transport Layer Security (TLS) protocol. For more information about connectivity, see the **Technical Connectivity Guide for SAP Cloud Applications**, which you can find on SAP Service Marketplace.

The server certificate used by the reverse proxy must be trusted by the SAP Cloud system.

You can download these certificates at *https://secure.omniroot.com/support/sureserver/rootcert.cfm*.

The communication channels for monitoring and maintaining instances of your SAP Cloud solution instances in the SAP data center network are also encrypted and authenticated.

Ensure that you also read the following relevant subsections:

- *Using Firewall Systems for Access Control* *Application-Level Gateways Provided by SAP* *Web Dispatcher*
- *Using Multiple Network Zones*

You can upload attachment files to your SAP Cloud solution in several application scenarios, for example in billing, in data migration, or image files of your travel expense receipts. Regularly updated antivirus software checks the uploaded files for viruses and other types of malicious software.

Recommendation

In addition to this antivirus software, we recommend that our customers also use antivirus software. Uploaded files are blocked based on their filename extensions, which can be manipulated.

In Business Configuration, you can define which file types can be uploaded to your solution. You should note that filename extensions can be changed to disguise the actual file format of the file.

4 Security Aspects of Data, Data Flow, and Processes

4.1 Communication Channels

The table below shows the communication channels used by SAP Cloud solutions, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Technology Used	Type of Data Transferred	Data Requiring Special Protection
Web browser acting as front-end client to access the hosted SAP Cloud solution system	HTTPS	REST services	Application data	User IDs, passwords
SAP Cloud for Travel and Expense to post financial data to customer ERP system File-based transfer of master data from customer ERP system to SAP Cloud for Travel and Expense	HTTPS	System-to-system connection	List of personal travel expenses (for financial reimbursement, taxation, and G/L posting) Master data (employees, cost centers, internal orders, projects, currency exchange rates, sales orders)	Expense report details Basic employee data, cost centers
Apple® iPad® application, Apple® iPhone®, BlackBerry® player, Android™, (SAP Business ByDesign, SAP Cloud for Customer, and SAP Cloud for Travel and Expense), Windows® Phone (SAP Business ByDesign)	HTTPS	REST services	Application data	User IDs, passwords, application data
E-mail	SMTP	SMTP server	Application data	Confidential data
Business-to-business communication and application integration	HTTPS	Web services	Application data	Application data

> **Note**
>
> SAP Cloud solutions use port 443 for HTTPS connectivity.

> **Caution**
>
> We strongly recommend that you use secure protocols such as Transport Layer Security (TLS) or Secure Network Communication (SNC).

4.2 Business-To-Business Communication and Application Integration

Business-to-Business (B2B) communication and application integration refers to the exchange of business-related data across administrative domains. These domains need not necessarily belong to different entities, such as companies; they can also represent different geographic subsidiaries of the same company.

Communication arrangements enable you to configure the electronic data exchange between your solution and a communication partner. A communication partner can be a business partner in a B2B communication scenario or an external communication system that is used for application integration, for example, external time recording or master data systems.

Your SAP Cloud solution provides communication scenarios for inbound and outbound communication that you can use to create communication arrangements. Inbound communication defines how business documents are received from a communication partner, whereas outbound communication defines how business documents are sent to a communication partner.

Before you can use electronic data exchange for a particular business process, you must configure and activate a communication arrangement for the corresponding communication scenario. You can do so during your solution configuration or, after configuration is complete, in the *Communication Arrangements* work center view in the *Application and User Management* work center.

You can find the list of trusted certification authorities for server certificates in the *Application and User Management* work center under *Common Tasks* *Edit Certificate Trust List*.

Security configuration for electronic data exchange is conducted at the communication arrangements level, where you can configure the authentication method and communication security.

Like end user authentication, B2B communication and application integration can be authenticated by two mechanisms: user ID plus password, and the X.509 client certificate. For inbound communication, you can upload the communication partner's client certificate in the configuration user interface, and map it to the communication user.

> **Caution**
>
> You can download an X.509 key pair from your SAP Cloud solutions. These key pairs are only intended for communication with the SAP Cloud solution and must not be used for other communication. This is because the corresponding certificate can be blocked in the solution and you can make the key pair invalid for logging on to the client but you cannot invalidate its other uses.

For outbound communication, you can upload a PKCS#12 container file, consisting of a private key and the corresponding client certificate that must be trusted and mapped by the communication partner. Administrators can monitor the validity of client certificates in the *Application and User Management* work center under *Common Tasks* *Edit Certificate Trust List*.

Certificates have a validity period and expire at a defined point in time. Before expiration, they must be renewed; if the client certificate's Subject or Issuer has changed, then the upload and mapping process must be repeated. Communication arrangements are the customer's responsibility, since their configuration reflects the specific details of their business partner. As a result, expiring certificates cannot be replaced automatically by SAP; this action must be performed by the customer.

A good security concept also includes mandatory periodic password changes. These changes must be performed synchronously by both parties involved. If an expired client certificate is renewed with the same attributes, the certificate information can be exchanged asynchronously.

Recommendation

We recommend authentication using Single-Sign on with SAML 2.0 for browser-based access and user names plus passwords for access from mobile devices. Please ensure that the passwords used are strong enough.

4.2.1 Integration of SAP Cloud for Travel and Expense with Other Components

Data flow and processes are handled as follows in a system landscape where SAP Cloud for Travel and Expense is integrated with other components:

- For IDoc-XML and Web service replication, data is encrypted using HTTPS protocol.
- File-based master data upload can be encrypted, except currency exchange rates.
- XLS file-based posting is not encrypted.

4.2.1.1 Security Mechanisms for the Exchange of Master Data and FI Expense Data Using Messages

The transfer of master data from the customer ERP landscape to SAP Cloud for Travel and Expense as well as the posting of expense reports is handled using IDoc XML messages or web services. The communication channels are encrypted using the HTTPS protocol.

Proper authorizations are required to execute the master data transfer steps on both sides.

4.2.1.2 Security Mechanisms for the Exchange of Master Data and FI Expense Data Using XLS/XML Files

The transfer of master data from your ERP landscape to SAP Cloud for Travel and Expense can also be handled using `.xml files` or `.csv` files. If you replicate from an SAP ERP system, the files can be encrypted at download

time and decrypted by SAP Cloud for Travel and Expense at upload time. Administrators manually control this process and need to provide passphrases for encryption. Ensure that you follow SAP guidelines for secure passwords.

> **Recommendation**
>
> We recommend that you use the file-based communication only if you cannot use IDoc messages or web services.

Proper authorizations are required to execute the master data transfer steps on both sides.

SAP Cloud for Travel and Expense also allows the transfer of accounting, reimbursement and taxation data using `.xls` files to non-SAP financial or HCM target systems, which typically accept only non encrypted data. These files are not encrypted at download time. Therefore, we strongly recommend that you ensure that .xls files for financial accounting are stored on encrypted file systems and handled with specific care with respect to security, that is, very restricted set of involved personnel, careful handling and deletion of transferred data files.

For more information, see the *SAP Cloud for Travel Integration Guide* on *SAP Service Marketplace* at *http://service.sap.com/instguides* *Installation & Upgrade Guides* *Cloud Solutions from SAP* *SAP Cloud for Travel and Expense*

4.2.1.3 Security Risk in the Communication with SAP ERP

The customer's SAP ERP system acts as a governing instance for SAP Cloud for Travel and Expense. Any manipulation of data during the upload process (during file-based replication or in the staging area) to SAP Cloud for Travel and Expense is very likely to be discovered because the original data resides in SAP ERP, and will result in data inconsistencies.

> **Example**
>
> FI expense posting errors will occur if you try to book on a non-existing cost center in SAP ERP or if you try to reimburse to a non-existing employee. You can also use regular reporting means to discover unauthorized transactions.

Personnel-related data is often critical. However, SAP Cloud for Travel and Expense only requires and stores very basic personal data, such as name, e-mail address, and employee ID/personnel number. The following information is neither required nor being transferred to SAP Cloud for Travel and Expense:

- Date and place of birth
- Salary
- Bank account data
- Passwords

> **Recommendation**
>
> As a system administrator, you must ensure that all transfer files are deleted securely after uploading the data to SAP Cloud for Travel and Expense.

For a detailed interface description that lists all mandatory and all optional data transferred to SAP Cloud for Travel and Expense, see the respective file on SAP Service Marketplace at: *https://service.sap.com/instguides* *Cloud Solutions from SAP* *SAP Cloud for Travel and Expense*.

4.2.1.4 Online Booking and Itinerary Management Tools

SAP Cloud for Travel and Expense uses a set of Web services provided by the online booking tool to enable automatic replication of booking data as well as approval workflow integration for itineraries.

The user and password for the technical user that is used for Web service authentication is maintained in the communication arrangement and securely stored, that is in Secure Storage of the communication arrangement.

The Web service is based on SOAP over HTTPS (data exchange is encrypted via SSL/TLS).

For the navigation from SAP Cloud for Travel and Expense to the online booking tool, a POST request over HTTPS is used.

SAP Cloud for Travel and Expense uses a set of Web services provided by the itinerary management tool to enable automatic replication of itinerary data.

As a prerequisite for the integration with Traxo, you must enable the client registration for OAuth web services by entering client ID and client secret as provided by Traxo in the Fine Tuning settings of SAP Cloud for Travel and Expense. For more information, see *SAP Cloud for Travel Integration Guide* *Integrating SAP Cloud for Travel with Traxo*.

Every user has to allow the system to replicate data on their behalf. When the user logs on to SAP Cloud for Travel and Expense, the system automatically replicates the itinerary data from the itinerary management tool to SAP Cloud for Travel and Expense. For the navigation from SAP Cloud for Travel and Expense to the itinerary management tool, a POST request over HTTPS / Oauth is used.

4.2.1.5 Credit Card Issuers

SAP Cloud for Travel and Expense uses a credit card Web service provided by Paymetric to enable the automatic and secure processing of expense-related credit card data, thereby ensuring that credit card data is handled in accordance with PCI security standards.

When SAP Cloud for Travel and Expense receives credit card transaction data from a credit card issuer, it does so through the Paymetric tokenization and file import Web service. This ensures cardholder numbers are intercepted and replaced with a token ID.

The Web service allows you to import credit card transactional data that is encrypted and stored in a centralized database maintained by Paymetric. The Web service then returns a token that is used in place of the sensitive data. The token is saved in your SAP Cloud for Travel and Expense database and can be used throughout your system.

The Web service is based on the standard Simple Object Access Protocol (SOAP v 1.1) protocol.

The Web service uses client certificates to identify the source of the Web service call. Paymetric provides you with instructions for generating a certificate signing request (CSR) that also generates a private key. You send the CSR

to Paymetric. Paymetric generates a certificate using the CSR and returns the signed client certificate (.csr file) to you. You save the signed client certificate and the private key to a secure location on a machine to which your client application has access. These files are then referenced in the SOAP header of your Web service calls.

4.2.1.6 Central Receipt Scanning and Electronic Invoices

SAP Cloud for Travel and Expense provides Web services for use by the third-party central receipt scanning service to enable automatic upload of receipt images to employee-related expense reports. In addition, it provides a Web service, *Electronic Invoice Notification*, for use by third-party service providers who want to send electronic invoices for travel expenses to SAP Cloud for Travel and Expense. The Web service is based on SOAP over HTTPS.

Certificates for third-parties are used for Web service authentication, and are maintained and securely stored in the relevant communication arrangement. It is recommended to use certificates for authentication. It is also possible to use a password.

The inbound Web service connection is authenticated with a client certificate to identify the source of the Web service call. Both the central receipt scanning service and the electronic invoice service have their own separate client certificates, and it is the responsibility of the third-party to provide the certificate to the system administrator of SAP Cloud for Travel and Expense for upload. The client certificate is saved to a secure location on the machine which the SAP Cloud for Travel and Expense solution accesses. These files are then referenced in the SOAP header of your Web service calls.

It is also the responsibility of the third-party to renew the certificate in time, send the SAP Cloud for Travel and Expense system administrator the renewed certificate, and choose a certificate authority trusted by SAP.

If no certificate is provided by the third-party, you can download it from the *Communication Arrangements* view in the *Application and User Management* work center.

4.2.1.7 Receipts

In SAP Cloud for Travel and Expense, travelers can upload receipts to be attached to the expense report.

The following formats are supported:

- .bmp
- .gif
- .jpg/.jpeg
- .pdf (not supported on smartphone devices)
- .png
- .tif/.tiff (not recommended and not supported on smartphone devices)

> **Note**
>
> The size for the above file types cannot exceed 6 MB.

4.2.1.8 Electronic Invoices

In SAP Cloud for Travel and Expense, third-party travel service providers can send electronic invoices to be assigned to travelers and to expense reports.

The following MIME types are supported for attachments:

- .gif
- .image/.png
- .jpeg
- .pdf
- .png
- .tiff (not recommended and not supported on smartphone devices)

> **Note**
>
> The size for the above file types cannot exceed 2,5 MB.

4.2.1.9 Smart Receipt Recognition

SAP Cloud for Travel and Expense enables the automated optical character recognition of receipt images sent to SAP Cloud for Travel and Expense by e-mail as attachments. Receipt images are analyzed to extract text relating to expense type, date, amount, and currency.

The data exchange between SAP Cloud for Travel and Expense and OpenText is based on SOAP over HTTPS (data exchange is encrypted via SSL/TLS).

The following MIME types are supported for smart receipt recognition:

- .gif
- .jpg/.jpeg
- .pdf
- .png
- .tif/.tiff

4.3 E-Mail

SAP Cloud solutions enable you to encrypt outgoing e-mails and check the signature of incoming e-mails by using the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. You can use this function for e-mail communication between your system and your employees, in e-mail scenarios provided by SAP (for example, self-service or approval scenarios). You can specify which e-mail scenarios you want to use in Business Configuration.

> **Caution**
>
> We strongly recommend that you only send encrypted mails and accept only signed e-mails.

The system uses the same certificate for signature check and e-mail encryption, which means that the same private key is used for signing and decrypting an e-mail to or from an employee.

The following MIME types are supported for e-mail communication with the system:

- .gif
- .jpg/.jpeg
- .pdf
- .tif/.tiff
- .png

> **Caution**
>
> When you use S/MIME, ensure that the data is encrypted. Please note that e-mail header data, for example, the subject line, is not encrypted. The sensitivity setting for password e-mails is set by default to private.

The following diagram provides an overview of how e-mail encryption and signature is set up:

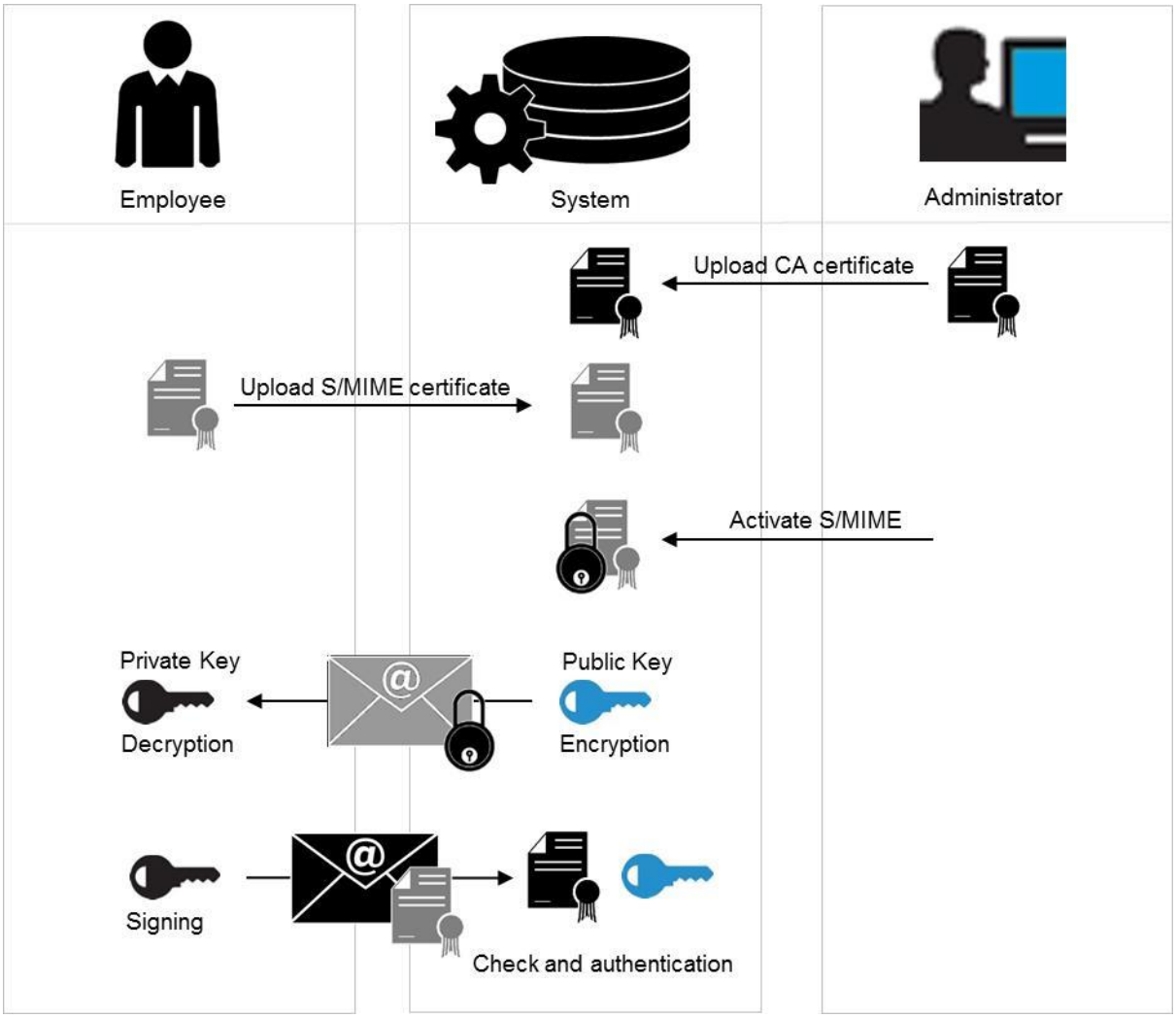


Figure 1: E-Mail Security with S/MIME

5 User Administration and Authentication

5.1 User Management

User management for SAP Business ByDesign and SAP Cloud for Travel and Expense is located in the Application and User Management work center. User management for SAP Cloud for Customer is located in the Administrator work center.

The following table provides an overview of all activities related to user administration that you can perform as an administrator:

Table 2:

View	Subview	Activity	Documentation in the Help Center
Application and User Management (SAP Business ByDesign and SAP Cloud for Travel and Expense) *Administrator* (SAP Cloud for Customer)	Business Users	Lock and unlock users Change user password Edit the validity of a user Assign security policies to users Assign access rights to users for work centers and work center views Restrict read and write access for users to specific data Assign business roles to users	*Business Users Quick Guide*
	Support and Technical Users	View all support and technical users available in the system	
	Business Roles	Define access rights in business roles	*Business Roles Quick Guide*
Application and User Management (SAP Business ByDesign and SAP Cloud for Travel and Expense) *Administrator* (SAP Cloud for Customer)	Communication Arrangements	Create technical users for electronic data exchange	*Business Roles Quick Guide*
	Communication Certificates	Manage certificates that you use for electronic data exchange	*Personalize my Settings*

View	Subview	Activity	Documentation in the Help Center
Common Tasks (SAP Business ByDesign and SAP Cloud for Travel and Business Configuration (SAP Cloud for Customer)	Edit Security Policies	Specify security policies for user passwords	*Security Policies Quick Guide*
	Configure Single Sign On	Download service pro-IdP metadata, and activate SSO	*Configure your Solution for*
	Configure S/MIME	Configure and activate e-mail communication with S/MIME	*E-Mail Security Configuration: Load Certificates and Activate Signing and Encryption for E-Mails*
	Edit Certificate Trust List	Edit trust list of certificates used for communication arrangements **Note** The list of trusted certification authorities is available on the Web dispatcher. Certificates with which users log on must be issued by one of these certification authorities.	*Communication Arrangements Quick Guide*

For more information about how to perform these activities, see the documentation of the corresponding work center view.

5.2 User Types

SAP Cloud solutions provide the following user types:

User Type	Description
Business User	A user type for normal interactive users resulting from hiring an employee or creating a service agent. Business users always have to change their initial password during the first logon. The properties of the passwords are determined by the assigned security policy. Note Service agents are used for external users, for example, partners or partner contacts. Apply specific security policies and use specific roles to keep internal and external employees separated. We also recommend that you lock external users as soon as they are no longer needed.
Technical User	A user type for non-interactive usage, either predefined by SAP for technical operations or resulting from the creation of communication arrangements. Technical users either do not have passwords or have password but do not have to change them.
Support User	A user type for interactive support users used by SAP Cloud Services to access the system as part of incident processing.

It is often necessary to specify different security policies for different users. For example, your policy may mandate that individual users who perform tasks interactively change their passwords on a regular basis.

You can only specify security policies for the Business User user type.

5.3 Authentication Mechanisms

Every user type must authenticate itself to SAP Cloud solutions for regular browser-based front-end access, as well as for electronic data exchange, such as Business-to-Business communication. SAP Cloud solutions do not support anonymous access.

When a new user is created in your SAP Cloud solution, for example, during the hiring process of a new employee, a user ID is created.

To log on your SAP Cloud solution, the following authentication mechanisms are supported:

- Logon using SAML 2.0 assertion for front-end Single Sign-On (SSO)
- Logon using client certificate (X.509) as logon certificate
- Logon using user ID and password

5.3.1 Logon Using SAML 2.0 Assertion for Front-End Single Sign-On (SSO)

Your solution supports SSO based on Security Assertion Markup Language 2.0 (SAML 2.0). To use this function, your system landscape requires the following components:

- An SAML 2.0 enabled identity provider (IdP)
- At least one local service provider, for example, your solution or a Web-based 3rd-party product
- A browser client

The use of an SAML 2.0. enabled identity provider is mandatory. If you have no identity provider, it is recommended that you use SAP Identity Provider.

When a user connects to the service provider by using the corresponding URL, the browser redirects the authentication request to the IdP. If the user is not yet logged on, he or she is prompted to logon to the IdP. After that the browser redirects the connection back to the original URL and the user is automatically logged on to the service provider. This process flow is always the same for all server providers.

The mutual trust between service provider and IdP is established by the exchange of certificates and additional metadata.

For more information, see the *Front-End Single Sign-On* document in the Help Center and the SAP Identity Provider documentation on SAP Help Portal at *http://help.sap.com/netweaver* *SAP NetWeaver Identity Management* *<release>* *Application Help*.

5.3.2 Logon Using Client Certificate (X.509)

Users can also log on with a client certificate to complete authentication. To do so, users can choose between the following options:

- If users already possess a suitable client certificate from a trusted Certification Authority, then they can map the client certificate to their user ID.
- If no suitable client certificate is available, then users can request a client certificate from within the SAP Cloud solution. In response, an SAP Certification Authority will provide the requested certificate. This request can be repeated on any other device you use to access SAP Cloud solutions. You cannot use the same certificate to log on with multiple users.

We strongly recommend that you never store the X.509 client certificate in an unprotected keystore. The download also contains the corresponding private key. Therefore, the downloaded file should be protected with a sufficiently strong passphrase of the user's choice.

The following table contains the trusted certification authorities for client certificates:

Table 3: Trusted Certification Authorities

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
DE	Deutsche Telekom AG	T-TeleSec Trust Center	Deutsche Telekom Root CA 1	
DE	SAP Trust Community		SAP Passport CA	
DE	TC TrustCenter GmbH	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA II	
DE	TC TrustCenter GmbH	TC TrustCenter Universal CA	TC TrustCenter Universal CA I	
DE	TC TrustCenter for Security in Data Networks GmbH	TC TrustCenter Class 1 CA		certificate@trust-center.de
IE	Baltimore	CyberTrust	Baltimore CyberTrust Root	
US	Entrust.net	www.entrust.net/CPS incorp. by ref. (limits liab.), (c) 1999 Entrust.net Limited	Entrust.net Secure Server Certification Authority	
US	Entrust.net	www.entrust.net/Client_CA_Info/CPS incorp. by ref. limits liab., (c) 1999 Entrust.net Limited	Entrust.net Client Certification Authority	
US	Equifax	Equifax Secure Certificate Authority		
US	GTE Corporation	GTE CyberTrust Solutions, Inc.	GTE CyberTrust Global Root	
US	GoDaddy.com, Inc.	http://certificates.godaddy.com/repository	Go Daddy Secure Certification Authority	
US	The Go Daddy Group, Inc.	Go Daddy Class 2 Certification Authority		
US	VeriSign, Inc.	Class 1 Public Primary Certification Authority		

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
US	VeriSign, Inc.	Class 1 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 2 Public Primary Certification Authority		
US	VeriSign, Inc.	Class 1 Public Primary Certification Authority		
US	VeriSign, Inc.	Class 1 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 2 Public Primary Certification Authority		
US	VeriSign, Inc.	Class 2 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 3 Public Primary Certification Authority		

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
US	VeriSign, Inc.	Class 3 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 4 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 1 Public Primary Certification Authority	
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 2 Public Primary Certification Authority - G3	
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 3 Public Primary Certification Authority - G3	
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 4 Public Primary Certification Authority - G3	
US	VeriSign, Inc.	VeriSign Trust Network, (c) 2006 VeriSign, Inc. - For authorized use only	VeriSign Class 3 Public Primary Certification Authority - G5	

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
ZA	Thawte Consulting cc	Certification Services Division	Thawte Premium Server CA	premium-server@thawte.com
ZA	Thawte Consulting cc	Certification Services Division	Thawte Server CA	server-certs@thawte.com

For more information about trust configuration, see SAP Help Portal at *http://help.sap.com/netweaver* *SAP NetWeaver Platform* *<release>* *Application Help* *Function-Oriented View* *<language>* *Security* *User Authentication and Single Sign-On* *Integration in Single Sign-On (SSO) Environments* *Single Sign-On for Web-Based Access* *Using X.509 Client Certificates* *Using X.509 Client Certificates on the AS ABAP* *Configuring the System to Use the SAP Trust Center Service*.

5.3.3 Logon Using User ID and Password

Users log on to SAP Cloud solutions with their assigned user ID and password.

By default, a strong security policy for passwords is pre-configured in your solution, based on SAP's product security standard. You as an administrator can set an initial password and edit and create security policies according to the security requirements of your company.

For more information, see *Security Policy* [page 25].

If a user has forgotten the password, he or she can request a new one by using the password self-service on the logon screen. A dialog box is displayed where the user has to enter the workplace e-mail address. Provided this workplace e-mail address has already been entered for corresponding employee or service agent in your solution, an e-mail containing a security code is sent to this e-mail address.

The system then displays a dialog box where the user can enter this security code. Note that the security code is only valid in this dialog box. If the security code has been entered correctly, the system generates a new temporary password with which the user can log on to the system. The system immediately displays another dialog box requiring the user to change this temporary password.

5.4 Security Policy

You as an administrator can increase the security level, if desired, by editing and enhancing the security policy, for example, by changing the complexity and validity for all passwords, in accordance with your company´s security requirements.

You can also define the length of time after which mobile users must reenter the app password to log on to the system from a mobile device and the maximum number of times in succession a user can enter an incorrect password before mobile app data is deleted from the mobile device as well as other properties regarding the complexity of the password.

For more information about the app password, see *Secure System Access and Authentication*.

6 Authorizations

6.1 Authorization Assignment

You can assign authorizations to each employee who has a user ID in your solution.

Employees are assigned to org units within organizational management. The assigned org unit determines the functions that the employee can use.

Based on these functions, work centers and work center views are proposed for the users. Some business processes require that a work center view can only be assigned together with one or more other work center views. If you as an administrator assign such a work center view to a user, then your solution automatically assigns these additional views to the user.

In SAP Customer OnDemand, you can enable partner contacts to access your SAP system by creating a user ID separate from employees in your solution. Partner contacts are service agents, being used to give external employees system access. Partner contacts should be assigned with their own business roles to maintain limited access to your SAP system.

Caution

Creating user IDs for your business partners will allow outside access to your system.

6.2 Access Restriction

You can define whether a particular user has read or write access to data in a work center view.

Except for SAP Cloud for Travel and Expense. Here, you can only assign business roles that determine the authorization.

Your SAP Cloud solution provides the user with access to all of the business documents and Business Task Management items in that work center view.

You can restrict access to specific data on the basis of the access context assigned to the work center view in which the data appears.

Caution

It is important to be aware of the following dependencies when you assign work centers and views directly to users:

- Each work center view contains specific activities that can be carried out by a user with the necessary access rights for the view. When you assign a view or work center directly to a user, rather than assigning these through a business role, by default the user will have unrestricted read and write access to all the functions associated with the work center view.

- Additionally, in some cases the same activities can be carried out in multiple views. When you grant access rights, you should be aware that if there is a conflict, unrestricted access rights override any restrictions you have defined. For example, view A and view B both contain activity C. For view A, a user has unrestricted read and write access but for view B, the same user has read-only access. Because unrestricted access rights override restricted access rights, the user will actually have both read and write access to both views.

Recommendation

We recommend that you handle access rights by assigning business roles to users rather than by assigning work centers views directly to users. The advantages of assigning access rights through business roles are considerable:

- It eliminates the risk of a user accidently having authorizations to read or edit data to which he or she should not have unrestricted access.
- There is much less maintenance effort involved when you have to edit access rights, for example, after an upgrade. You only have to edit the access rights associated with the business role and not the individual user's access rights.

6.3 Segregation of Duties

If the user has been assigned to multiple work centers, your SAP Cloud solution checks whether the assigned views conflict with the segregation of duties.

Segregation of duties is designed to minimize the risk of errors and fraud, and to protect company assets, such as data or inventories.

The appropriate assignment of access rights distributes the responsibility for business processes and procedures among several users.

For example, suppose that your company requires that two employees be responsible for the payment process. This requirement ensures that the responsibility for managing company finances is shared by two employees.

A segregation of duties conflict occurs when a user has access to a set of work center views that could enable him or her to make an error or commit fraud, thereby damaging company assets. If the application detects a conflict, it indicates that conflict in the user interface and proposes possible solutions.

Based on this information, you can alert business process owners to existing conflicts, so that they can implement process controls to mitigate them.

Users can define their own conflicts in addition to the ones delivered by SAP. The conflicts defined by SAP can be overridden or disabled.

7 Mobile Applications

7.1 General Information

The following table provides information about the mobile devices on which you can run SAP Cloud solutions.

SAP Cloud Solution	Device/Operating System				Offline Support
	iPhone/iPad	Blackberry	Android	Windows Phone	x
SAP Business ByDesign	x	x	X	x	x
SAP Cloud for Customer	x	x	x	x	x
SAP Cloud for Travel and Expense	x	x	x	x	x *

* SAP Cloud for Travel and Expense supports offline mode for Android, iPhone, Blackberry, and Windows Phone, but not iPad.

With the SAP Cloud mobile solutions, you can access many of the functions that have been tailored to business on-the-run. Changes made on mobile apps are automatically updated in the system over the Internet, online, and in real time. Mobile apps connect to the SAP Cloud solution in the same way as personal computers do.

7.2 Mobile Apps

You can download the mobile apps for SAP Cloud solutions from the respective stores as follows:

- Download the app for your SAP Cloud solution for the Apple® iPhone® or iPad® from the iTunes Store®. A notification will be displayed on-device when a new version of the app is available for download.
- Download the app for your SAP Cloud solution for BlackBerry® Curve™ and Bold™ smartphones running software versions 5.0 to 7.x from BlackBerry App World™. If necessary, the app can also be manually downloaded to a computer from the SAP Cloud solution system. If the app is manually installed on a BlackBerry smartphone, users will not be prompted to upgrade when a new version becomes available for download.
- Install the app for your SAP Cloud solution for Android® smartphones from the Google Play Store™. A notification will be displayed on-device when a new version of the app is available for download.
- Install the SAP Business ByDesign and SAP Cloud for Travel and Expense app for the Windows® Phone smartphone from the Windows® Phone Marketplace. A notification will be displayed on-device when a new version of the app is available for download. Install the SAP Mobile Execution app for Windows® Mobile from

SAP Business ByDesign. For more information, see the device manufacturer's documentation. App help is available on-device.

Caution

If the app is manually installed on a BlackBerry smartphone, users will not be prompted to upgrade when a new version becomes available for download.

7.3 Authorizations

When you use SAP Cloud mobile solutions, you use the same URL address and logon credentials as for desktop applications.

In the *Application and User Management* work center, ensure that for each mobile work center view to be accessed on a mobile device, the user of the mobile device is assigned the related desktop work center view. For more information, see the *Business Users Quick Guide* in the Help Center from any work center.

7.4 Secure System Access and Authentication

Access from mobile devices via the native mobile apps or the device browser (HTML5) is enabled by connecting to the back-end system using HTTPS and the same user and password authentication used for connection from a personal computer. To allow users to use their mobile devices in offline mode, you must enable the use of an app or offline password and define additional security settings for those passwords.

7.5 Password Change and Password Reset

On application level, you can either change or reset your app password. To change your app password, you must first enter your current app password. If you forgot your app password, you must reset it. Please note that in this case, your data (logon credentials and not synchronized expenses) is deleted.

On server level, you can reset your password by entering your e-mail address. Please note that your data is not deleted.

7.6 Special Considerations

Unlike stationary personal computers, mobile devices are at greater risk of being lost or stolen. Therefore, we recommend that you use the security features provided by your mobile device platform. For example:

- Use an additional, sufficiently long, PIN (personal identification number) to lock the device.
- Enable remote management software that allows you to lock the device remotely, or wipe data from it.

For information on how to operate your mobile device, refer to the device manufacturer's documentation.

7.7 Data Storage

The mobile apps for SAP Cloud solutions store three types of data on the mobile device, as outlined below.

7.7.1 Password Retention

When logging on to the SAP Cloud solution from a mobile app, the user is required to provide the user ID and system password. For SAP Business by Design and SAP Cloud for Customer, the mobile app does not store this data by default, but the user can change this setting by defining an app password. For SAP Cloud for Travel and Expense, the administrator has to configure a security policy. This security policy defines whether or not the user can set up an app password.

In this case, the user ID and system password are encrypted and stored on the mobile device, using the secure storage features provided by the operating system of that device. The app password itself, however, is not stored on the mobile device, but is used to retrieve the stored user ID and system password when connecting to the SAP Cloud solution from it.

As an administrator, you can specify the length of time after which the mobile user must reenter the app password to log on to the system. For SAP Cloud for Travel and Expense apps, the administrator also defines whether the user can set up an app password in the security policy. For more information, see Security Policy.

7.7.2 Support Log Files

To obtain support for a technical error within the mobile app, you may be requested to activate the app's error-logging functionality. When error logging is active and the technical error is reproduced, files containing technical data are created. These files enable SAP Cloud Support representatives to resolve the error. Delete the log files once they are no longer required.

Note

This section does not apply to SAP Cloud for Travel and Expense.

7.7.3 Cache Files

To improve the mobile app's performance, metadata is stored on your mobile device. The cached information contains technical data that describes the user interface. The cache files can be deleted.

For device-specific instructions on how to set the password expiration, enable logging, or delete logs and cache files, refer to the mobile app's documentation.

It is sometimes possible to upload pictures and other files from the mobile device to the SAP Cloud solution, for example, pictures captured on a mobile phone's camera. Such files are not managed through the SAP mobile app. When files are uploaded to the solution, they are not deleted from the mobile device. To protect any sensitive or confidential data that such files may contain, we recommend that you take extra precautions appropriate for the specific mobile device in use. For more information, see the device manufacturer's documentation.

For device-specific instructions on how to set the password expiration, enable logging, or delete logs and cache files, refer to the mobile app's documentation.

You can upload pictures and other files from the mobile device to the SAP Cloud solution, for example, pictures captured on a mobile phone's camera. Such files are not managed through the SAP mobile app. When files are uploaded to the solution, they are not deleted from the mobile device. To protect any sensitive or confidential data that such files may contain, we recommend that you take extra precautions appropriate for the specific mobile device in use. For information on how such files are secured and stored on your mobile device, refer to the device manufacturer's documentation.

7.7.4 Offline Mode

Data is stored on the device and encrypted. Once the device is online, data sent to the back-end system, synchronized, and deleted from the mobile device.

For working offline, data is stored on the device and encrypted.

For mobile apps, once the device is online, data is sent to the backend system, synchronized, and deleted from the mobile device.

> **Note**
>
> This section only applies to the mobile apps for SAP Business ByDesign, and the SAP Cloud for Travel and Expense apps for iOS and Blacklberry.

7.7.5 Local Application Data Storage

SAP Cloud for Customer supports local application data storage. To enable this, you first have to log on to the SAP Cloud for Customer system and enter user name, online password, and system URL. During the setup, the user has to enter an offline password that is different from the online password. The local application data has been

encrypted with a key derived from the offline password. Authentication is required to switch between online and offline mode.

8 Front-End Security

The SAP Cloud solutions front ends consist of Web application user interfaces based on Microsoft ® Silverlight™ or HTML5 technology.

8.1 Microsoft ® Silverlight™

Microsoft ® Silverlight™ is a development platform for Web applications.

You can run Microsoft ® Silverlight™ applications in your Web browser and benefit directly from the browser´s security mechanisms. Examples of browser security mechanisms are secure cookie handling and same-origin policy. The same-origin policy ensures that confidential data is exchanged only with the domain of origin and that it is not stored on the client after the current session ends.

Microsoft ® Silverlight™ applications from different domains of origin run independently of one another. They do not share resources, such as business data. The applications have very limited access to the client's resources, such as the local file system.

The user interface of your SAP Cloud solution benefits from the following front-end security mechanisms and concepts:

- Microsoft ® Silverlight™ application sandbox and resource isolation
- Transport Layer Security (TLS) encryption using HTTPS
- Access to business data only after authentication and with sufficient authorizations using identity management and Role-Based Access Management (RBAM)
- Cross-site-scripting countermeasures
- Microsoft's secure default configuration in the framework
- Secure Web Application Development Guide

For more information, see the security information for Microsoft ® Silverlight™.

8.2 HTML5

HTML is a markup language for the Web. HTML allows you to format text, add graphics, create links, input forms, frames and tables, and save it all in a text file that any browser can read and display. HTML5 is the latest version. It offers enhanced multimedia capabilities.

> **Note**
>
> HTML5 has been released for SAP Cloud for Customer and SAP Cloud for Travel and Expense only.

In addition to the features that are also supported by Microsoft ® Silverlight™, HTML5 supports the following features:

- X-Frame-options response header to avoid clickjacking attacks

- Cross-site request forgery (CSRF) protection
- Cross-site scripting (XSS) output encoding during SAP UI5 rendering
- UI and domain protection against URL mashups and content mashups in iFrames

For more information, see the security information for HTML5.

9 Security of Data Storage and Data Centers

The data centers that support SAP Cloud solutions incorporate multiple safeguards for physical data security and integrity. They also provide high availability of your business data, using redundant networks and power systems.

9.1 Asset Protection and Data Integrity

SAP follows operating best practices for data centers by deploying computation and storage parts of the solution over separated fire-safe areas to support disaster recovery in the event of a fire.

For data backup and recovery purposes, a redundant hardware storage system performs regular backups. To provide enhanced data integrity, your SAP Cloud solution uses an advanced database management solution to store customer data and securely isolate each customer's business information in its own database instance.

9.2 Power Backup and Redundancy

SAP data centers maintain multiple connections to several power companies, making a complete power outage highly unlikely. Even if the local power grid were to fail, the data centers supporting your SAP Cloud solution have an uninterruptible power supply for short-term outages, and a diesel generator backup power supply for longer-term outages. Therefore, power interruptions or outages are unlikely to affect customer data or solution access.

9.3 Restricted Physical Access

SAP data centers, located in the United States of America and Germany, are logically separated and staffed around the clock, 365 days a year. A biometrics security system permits access only to authorized personnel, and the data centers are partitioned such that authorized personnel can access only their designated areas. Moreover, no direct network connection exists between individual SAP data centers; each SAP data center is fully autonomous.

9.4 Communication Security

SAP relies on encryption technology that uses HTTPS to prevent unauthorized parties from intercepting network traffic. The encryption is based on the Transport Layer Security (TLS) protocol. The required encryption software is a standard component of up-to-date client operating systems and Web browsers.

9.5 Network Security

The network for your SAP Cloud solution employs a number of security technologies. The multilayered, partitioned, proprietary network architecture permits only authorized access to the data centers that support your SAP Cloud solution, with features that include:

- A Web dispatcher farm that hides the network topology from the outside world
- Multiple Internet connections to minimize the impact of distributed denial-of-service (DDoS) attacks
- An advanced intrusion detection system that continuously monitors solution traffic for possible attacks
- Multiple firewalls that divide the network into protected segments and shield the internal network from unauthorized Internet traffic
- Third-party audits performed throughout the year to support early detection of any newly introduced security issues

10 Security for Additional Applications

SAP offers a set of additional software components that you can install, on desktop computers, for printing and additional functionality.

10.1 Confirm the Signature

All additional applications of SAP Cloud solutions that are delivered for download are digitally signed. To confirm the signature, proceed as follows:

1. Right-click on the file you have downloaded, then choose *Properties*.
2. In the dialog box, choose the *Digital Signatures* tab.
3. Confirm that the indicated *Name of signer* is SAP AG.

When you execute the installation of a file, a popup appears, indicating the *Verified publisher*. In this case, SAP AG is indicated as well.

10.2 Saving Logon Data

SAP front-end components never share an existing authentication session on SAP Cloud solutions, for example, within a Web browser or with another front-end component. Dedicated authentication is always required to build a confidential communication channel, secured via the Transport Layer Security (TLS) protocol, to your SAP Cloud solution.

If you log on to the system from a desktop computer with a user ID and password, you are asked whether you want to store the password locally for subsequent authentication purposes. The password is encrypted, and not stored as plain text. It is stored using the available protection mechanisms of the operating system, and can be reused only by the operating system user who is currently logged on. If you do elect to use this function, then you should activate it on your device only, and never on public computers.

11 Other Security-Relevant Information

11.1 Service Composition Security

This section describes security considerations that apply to the built-in mashups integration and Web services composition capabilities of SAP Cloud Solutions. Mashups and service composition entail cross-domain communication between various Internet domains.

Content from different domains – especially active content, such as JavaScript – is always domain-separated in the Web browser.

A same origin security policy common in Web browsers, prohibiting access to content across domain separations, is activated, if necessary.

11.1. URL Mashup Integration

Both partners and administrators can create URL mashups to perform the following tasks:

- Open a Web page.
- Open a resource, for example, a Microsoft® Office or Adobe® PDF document, an Adobe® Flash® or multimedia video file, and so on.
- Open a custom URL of a front-end application, for example, Microsoft® Outlook®, Apple iTunes®, and so on.

You can open these items from an SAP Cloud solution screen by configuring the URL with dynamic parameters that are derived from the screen out-port interface of your SAP Cloud solution.

Caution

Some URLs may pass your business data to an external application provided by a third-party organization, for example, account data passed to a search engine when performing a reverse lookup in an online address book. Therefore, before you use the URL mashup, we recommend that you confirm that it conforms to your company's security and data privacy policies.

Some Web browser settings, for example, popup blockers, may prevent the new browser window from appearing in the URL mashup. We therefore recommend that you review your browser settings to determine whether popups are allowed.

11.1.2 HTML Mashup Integration

Both partners and administrators can create HTML mashups to embed an HTML-based Web page or a resource that can be rendered in a Web browser – for example, a Microsoft Office or Adobe PDF document, or an Adobe

Flash or multimedia video file – into an SAP Cloud solution screen by configuring the URL with dynamic parameters that are derived from the SAP Cloud solution screen out-port interface.

Caution

Certain URLs may pass your business data to an external application provided by a third-party organization, for example, account or contact data passed to a social media Web site when displaying the related profile. Therefore, before you use the map mashup, we recommend that you confirm that it conforms with your company's security and data privacy policies.

Bing Maps Web service communication takes place directly between the user's Web browser and the service provider via the Transport Layer Security (TLS), with the dedicated API key applied for each SAP Cloud solution. Bear in mind that the Bing Map Web service provider may monitor the Bing Maps Web service API usage in accordance with the terms of licensing. Therefore, before you use the map mashup, we recommend that you review the API usage and licensing details with the Bing Maps Web service provider.

11.1.3 Map Mashup Integration

SAP Cloud solutions use Microsoft® Bing Maps™ as a built-in map service provider. Both administrators and end users can configure the map mashup usage on an SAP Cloud solution screen to display the visual location or route information on a map. Before Bing Maps mashups can be used, you as an administrator must activate them by entering the Application Programming Interface (API) key for Bing Maps usage in the *Mashup Authoring* work center view of the *Application and User Management* work center. For more information about the Bing Maps Web service partner, and to apply for an API key, visit the SAP Cloud solutions communities.

Caution

Bear in mind that the map mashup may convey business data of yours to the Bing Maps Web service provider. For example, ship-to and bill-to addresses are transferred to the Bing Maps Web service provider when displaying the related visual location on the map. Therefore, before you use the map mashup, we recommend that you confirm that it conforms with your company's security and data privacy policies.

Bing Maps Web service communication takes place directly between the user's Web browser and the service provider via the Secure Sockets Layer (SSL), with the dedicated API key applied for each SAP Cloud solution. Bear in mind that the Bing Map Web service provider may monitor the Bing Maps Web service API usage in accordance with the terms of licensing. Therefore, before you use the map mashup, we recommend that you review the API usage and licensing details with the Bing Maps Web service provider.

11.1.4 Data Mashups

Both partners and administrators can create data mashups for composing Web services (provided by third-party Web service providers) with business data derived from the SAP Cloud solutions. You can use the integrated authoring tool, the Data Mashup Builder, to transform or merge external Web services with internal business data, using industry-standard Web service protocols, for example, RSS/Atom, REST or SOAP Web services.

Create Web services in your SAP Cloud solution before creating the Web service composition in the Data Mashup Builder. API keys can be specified for the Web service security by means of industry-standard or Web service specific authentication methods, for example, basic authentication, REST body credentials, or SOAP service parameter credentials. The API keys entered by partners and administrators are stored in an isolated secure storage of your SAP Cloud solution back end, which is never exposed to end users.

Caution

Certain Web services may transfer business data of yours to an external Web service provider from a third-party organization. For example, account or address data is transferred to a data quality Web service provider when data quality cleansing operations in Cloud applications are performed. Therefore, before you use the mashup, we recommend that you confirm that the Web service conforms to your company's security and data privacy policies.

Web service communication in data mashups does not take place directly between the user's Web browser and the Web service provider. Rather, as a result of the cross-domain access policy restriction, it is tunneled using the SAP Cloud solution system back-end Web service proxy. Only the Web service endpoints that have been confirmed with acknowledgement by partners and administrators can be accessed by the SAP Cloud solution system back-end Web service proxy by all end users of a customer. Therefore, before you confirm that a Web service is added to your SAP Cloud solution, we recommend that you ensure that it conforms to your company's and country's security policies.

11.2 Internal and External Audits

SAP is committed to third-party validations, standards, and certifications of the policies and procedures we use to maintain our customers' security, privacy and data integrity. SAP maintains several certifications and accreditations to ensure that we provide the highest standards of service and reliability to our customers. SAP will continue efforts to obtain the strictest of industry certifications in order to verify its commitment to provide secure and reliable services.

For more information, see the security and standard accreditations on the Business Center for Cloud Solutions from SAP, at: *www.sme.sap.com/irj/sme/solutions?rid=/webcontent/uuid/30f7e866-fe58-2c10-5780-f056f2d71ed2&language=en*

The *Audit* work center helps external and internal auditors conduct an audit for a company. It provides you with read access to all information that is relevant for an audit, such as financial reports, master data, documents and document flow, as well as user and access rights. The system provides this information through a selection of reusable views from other areas. Unlike other work centers, the *Audit* work center permits read access only. You cannot perform any changes there.

All planning, follow-up activities, reporting of audit results, and findings must be completed outside your SAP Cloud solution.

The *Audit* work center provides the following information:

- General Ledger
- Fixed Assets
- Cost and Revenue

- Inventory Valuation
- Receivables
- Payables
- Liquidity Management
- User and Access Management

For more information, see the documentation of the *Audit* work center.

11.2.1 Security Management and Continual Improvement of Security

Security Management at SAP Cloud Solutions aims towards the continual improvement of the information security framework. SAP conducts several external audits to make sure that these aims are reached.

Certificate/Report	Interval	Conducted by
ISAE-3402/SSAE-16 (Business By-Design)	Twice a year	External accounting company
ISO 27001 (SAP Cloud Operations)	Once a year	Accredited auditing company
ISO 27001 (SAP Data Center Operations)	Once a year	Accredited auditing company
External pentest	Twice a year (SAP Business ByDesign) Every major release (SAP Cloud for Customer)	Third-party security company
Internal pentest	Twice a year (SAP Business ByDesign) Once a year (SAP Cloud for Customer)	SAP C.E.R.T.
Code Scan ABAP (SAP Cloud for Customer) Non-ABAP (SAP Cloud for Customer)	Every major release (SAP Business ByDesign) ABAP: Daily (SAP Cloud for Customer) Non-ABAP: Each release (SAP Cloud for Customer)	External code scanning company
BS25999 (SAP Data Center Operations)	Once a year	Accredited auditing company

12 Security-Relevant Logging and Tracing

12.1 Data Privacy

Data processing systems store master data or transactional data used to perform business processes and to document them. In many cases, this is personal data relating to employees or other private persons. In many countries, the storage, processing, disclosure, and deletion of such personal data from data processing systems must be in accordance with statutory data protection laws. One requirement in many countries is that such personal data can only be stored if a clear business reason exists for the retention of this data. Most data protection laws mandate that data is deleted after the business reason has expired. Alternatively, data can be anonymized rather than removed completely.

In addition, legislation in many countries stipulates that organizations must disclose the personal data stored on an individual, if the individual expressly requests it.

The Data Privacy Management work center allows those responsible for data protection matters within an organization to respond to and fulfill requests for the following in relation to the personal data of employees and customers:

- Disclose personal data relating to employees and private persons
- Remove employee personal data once the retention period for all relevant data has expired
- Monitor and manage automatic data removal processes using an application log
- Display log data detailing each access made to the Disclose Employee Data and Remove Employee Data overview screens

12.2 Security-Relevant Reports

The Application and User Management work center offers a set of reports that provide insight into the system´s behavior. Depending on your authorizations, not all of those reports may be accessible.

The following reports are provided:

- Access Rights Change Log
  This report displays a list of all users in the system and their assigned access rights. It also lists when and how the access rights were changed, and by whom. This information is relevant for compliance reasons, enabling you to monitor the system to prevent fraud, or to trace who made system changes, if fraud has been committed.
- All Current Access Rights
  This report displays a list of all users in the system, and the access rights currently assigned to them. This information is relevant for compliance reasons, enabling you to monitor the system to prevent fraud.
- All Current Users
  This report displays a list of all users in the system. This information is relevant for compliance reasons, enabling you to monitor the system to prevent fraud.

- Segregation of Duties (SOD) Conflicts Report
  This report displays the list of segregation of conflicts existing between assigned views of the business users. Segregation of duties is designed to minimize the risk of fraud and errors, and protect company assets such as data or inventories. This information is relevant for compliance reasons, enabling you to monitor the kind of authorizations you have for the users in your system and to make you aware of the kind of conflicting authorization assignments for any of the users.
- User Activation and Deactivation Log
  This report displays a list of all users in the system, and when they were activated or deactivated. This information is also relevant for compliance reasons, enabling you to monitor the system to prevent fraud.

Also in the User and Access Management work center, the IT Compliance view displays a list of IT control processes and allows you to monitor service provider access to your solution. IT control processes are IT-related changes made in your system, such as software updates or processes involving incident analysis.

13 Important Disclaimers on Legal Aspects

This document is for informational purposes only. Its content is subject to change without notice, and SAP does not warrant that it is error-free. SAP MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OR OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP specifically disclaims any liability with respect to this document and no contractual obligations or commitments are formed either directly or indirectly by this document.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. Regarding link classification, see: http://help.sap.com/disclaimer.