PUBLIC
2021-08-19

SAP Multi-Bank Connectivity

THE BEST RUN SAP

Content

1 SAP Multi-Bank Connectivity

Product Overview [page 3]	Provides an overview of the capabilities and concepts.
SAP Multi-Bank Connectivity Security Datasheet [page 39]	Provides a summary of the security features.

1.1 Product Overview

SAP Multi-Bank Connectivity is an on-demand solution that connects financial institutions and other financial service providers with their corporate customers on a secure network owned and managed by SAP.

SAP Multi-Bank Connectivity is based on integration services deployed in the SAP Cloud that enable the integration of business processes spanning different departments, organizations, or companies.

1.1.1 About SAP Multi-Bank Connectivity

SAP Multi-Bank Connectivity is an innovative on-demand solution that connects financial institutions and other financial service providers with their corporate customers on a secure network owned and managed by SAP. The network offers multiple services in one single channel while supporting the deployment of new services. As key benefits, the solution simplifies connectivity, automates financial transactions, reduces payment rejection rates, eases reconciliation, and provides enhanced visibility to corporate treasury.

> **i** Note
>
> As an example, let us look at a corporation with relationships with multiple financial service providers. SAP Multi-Bank Connectivity enables this corporation to establish a communication channel with these financial service providers, and to request payment order processing, for example, for paying salaries to its employees. The exchange of financial messages (for example, payment messages, status notifications or account statements) between the corporation and the corresponding financial service providers is handled by SAP Multi-Bank Connectivity.

When a financial institution and corporation want to connect, they first need to register to SAP Multi-Bank Connectivity and complete the onboarding process. Once they are onboarded and the counterparty that the newly onboarded customer wishes to connect to is identified, a service activation process takes place to connect the two. This is done for each connection required. The connected parties can then commence the exchange of messages across the network.

In addition, SAP Multi-Bank Connectivity provides connectivity to SWIFT via a managed service. In this scenario SAP operates SWIFT infrastructure and provides this as a service to the users of SAP Multi-Bank Connectivity.

SAP Multi-Bank Connectivity supports integration capabilities such as content-based routing and mapping, as well as certain connectivity options.

> **i Note**
>
> This document provides an overview of the capabilities and concepts of SAP Multi-Bank Connectivity and an overview of the security-related aspects.

Summary of Benefits Provided by SAP Multi-Bank Connectivity

SAP Multi-Bank Connectivity provides the following benefits:

- Pay-as-you-go subscription model
- Faster onboarding of financial institutions and corporations
- Embedded SWIFT connectivity
- Reduced operational risk
- Better visibility and control
- No additional cost for maintaining hardware and software
- Lower total cost of ownership (TCO)
- Standardized integration between financial institutions and their customers

1.1.2 SAP Multi-Bank Connectivity from a Bird's Eye Perspective

SAP Multi-Bank Connectivity is an integration platform that enables multiple participants (financial service providers and their corporate customers) to exchange financial messages (for example, payments, collections, status notifications, payment advices and account statements) in a reliable and secure way.

For each participant connected to SAP Multi-Bank Connectivity, separate resources (memory, CPU, and file system) are allocated in the SAP Cloud Platform. In the runtime of an SAP Multi-Bank Connectivity scenario, these resources are referred to as *tenants*.

For a corporate customer, SAP provides a Connector for SAP Multi-Bank Connectivity, S/4HANA on-premise and S/4HANA Cloud. This connector fully automates the communication with the relevant processes, such as a payment approval and triggers secure communication with the tenant of that customer in SAP Multi-Bank Connectivity. On the reverse flow, the connector triggers actions with the SAP ERP system which corresponds to the type of the message. For example, a status of a payment is updated or an account statement import is triggered.

Let us assume that two participants (*participant 1* and *participant 2*) exchange financial messages with each other through SAP Multi-Bank Connectivity. *Tenant 1* is allocated to (assigned to) *participant 1*, and *tenant 2* is assigned to *participant 2*. The exchange of data through SAP Multi-Bank Connectivity then works in the following way:

1. Participant 1 sends the financial message to tenant 1.
2. Tenant 1 forwards the message to tenant 2.

3. Tenant 2 sends the message to participant 2.

The communication paths between the participants and the tenants of SAP Multi-Bank Connectivity can be configured in a way that secure data transfer is guaranteed. In addition, the communication between the tenants (communication path 2 within the SAP Multi-Bank Connectivity platform) is also secured by SSL transport layer security besides the direct connection from a corporate customer to their financial institutions via SAP Multi-Bank Connectivity.

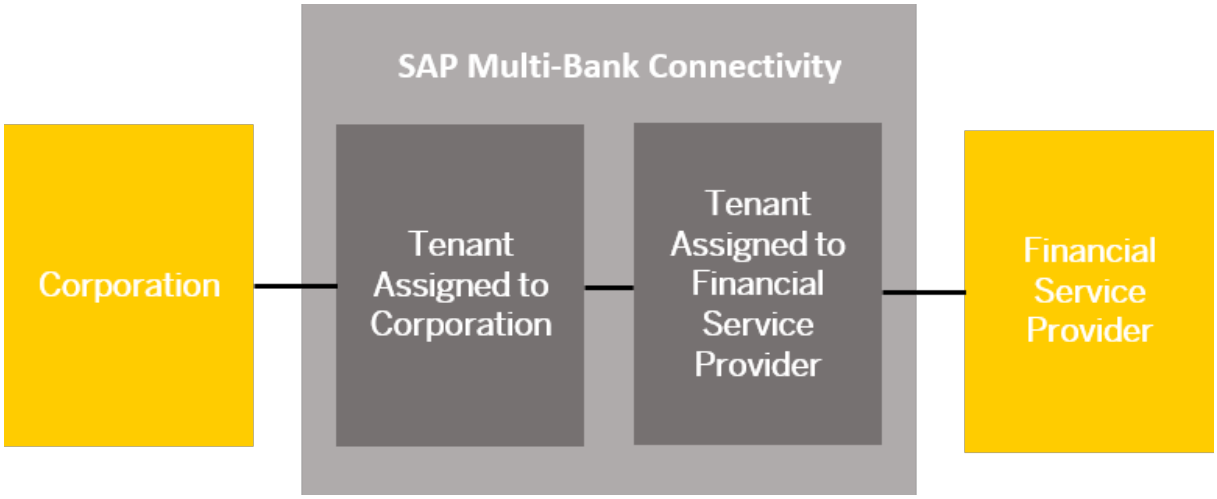
> **i Note**
>
> SAP Multi-Bank Connectivity is designed in such a way that each tenant uses a separate database schema. As a result, data isolation among the different participants using SAP Multi-Bank Connectivity is also ensured.

The figure given below illustrates this concept.

SAP Multi-Bank Connectivity offers an integration via SWIFT using SWIFT Alliance Lite. In this setup the exchange of data through SAP Multi-Bank Connectivity works in the following way:

1. Participant 1 sends the financial message to tenant 1.
2. Tenant 1 forwards the data to an SAP managed SWIFT infrastructure.
3. SWIFT forwards financial message to the financial institution.

The same communication is available in the other direction.



1.1.3 Capabilities

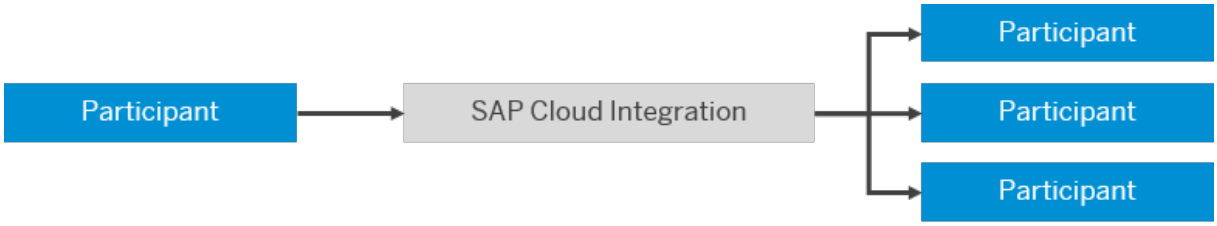
1.1.3.1 Integration Capabilities

There is a wide range of integration capabilities that define different ways how messages can be processed on the integration platform and exchanged between sender and receiver systems.

> → Remember
>
> There are currently certain limitations when working in the Cloud Foundry environment. For more information on the limitations, see SAP Note 2752867.

SAP Cloud Integration supports various integration patterns, or ways how applications can be integrated with each other.

The following figure illustrates, as one example, the routing pattern, that allows you to forward a message from one participant to multiple receivers.



When using SAP Cloud Integration, you specify the desired integration pattern by adding a dedicated **integration flow step** or a combination of various integration flow steps to an integration flow.

The following table lists the available integration capabilities, arranged by the related integration flow step types.

Message Transformation

Feature	Description
Mapping	Transforms the data structure and format used by the sender into a structure and format that the receiver can process. Supports the following kinds of mappings: • Message mappings designed with a graphical editor as part of the Cloud Integration tool-set (supports XSD and EDMX structures) • Custom-mapping functions defined in scripts • XSLT mappings (defined in an XSLT resource)
Converter	Transforms an input message into another format. The following converters are available: • Certain constraints apply with regard to the supported data formats (as described in the product documentation).
Decoder	Decodes the incoming message to retrieve the original data (for example, if a base64-encoded message has been received).

Feature	Description
Encoder	Encodes the message using an encoding scheme to secure any sensitive message content during transfer over the network.

Calling External Systems or Subprocesses

Routing

Feature	Description
Router	Routes a message to one or more receivers. SAP Cloud Integration also supports routing that depends on the content of the message (content-based routing). For example, the tenant detects that a message has a particular field value, and forwards it to the specific receiver participant that handles requests from the sender participant.
Multicast	Sends the same message to more than one receiver. • Parallel multicast: Initiates message transfer to all the receiver nodes in parallel • Sequential multicast: defines the sequence in which the message transfer to the receivers is initiated.
Splitter	Decomposes a composite message into a series of individual messages and sends them to a receiver. Supported splitters: Certain constraints apply with regard to the supported data formats (as described in the product documentation).

Storing Data During Processing

Feature	Description
Data Store Operations	Stores messages temporarily for later processing. The following operations are supported:

Protecting Messages

Feature	Description
Encryptor	Encrypts the content of a message. Supported standards:
Decryptor	Decrypts the content of a message. Supported standards:

Feature	Description
Signer	Signs a message. Supported standards:
Verifier	Verifies a message. Supported standards:

> **i** Note
>
> For mappings, XSLT (Extensible Stylesheet Language Transformations) 2.0 is supported.

> **i** Note
>
> Automatic stream caching mechanism is enabled to support streaming of large data and to avoid out-of-memory problems. This caching mechanism adds an interceptor between two processors, and caches streams either in memory or, if the stream is larger than 64 KB, in the file system. Hence enabling the streams to be read several times from the cache with reduced memory consumption .

Mapping

Mapping transforms (maps) sender into receiver data structures.

In scenarios spanning different application systems or different organizations and enterprises, it is very likely that the structure of the data exchanged between two participants will differ on both sides of a connection due to business-related reasons. To enable a seamless exchange of data, the data structures on both sides of a connection have to be transformed (or: mapped) into each other. There is the option to apply structural mapping of XML documents.

You can re-use existing on-premise content (service interfaces / message mappings / operation mappings / XSLT based mappings) from an SAP Enterprise Services Repository (EHP 1 for SAP NetWeaver 7.3).

Value mappings allow you to map different representations of an object to each other.

Value mappings are useful when performing a dynamic value lookup of an object that has different representations in different contexts. In value mappings, you map these different representations of an object to each other by setting mapping rules in a value mapping table.

> **i** Note
>
> For example: You can use a value mapping to map a Merchant ID to a Customer ID, where Merchant ID is an external application representation of a customer, while Customer ID is an internal SAP representation.

1.1.3.2 Connectivity (Adapters)

You have the option to specify which technical protocols should be used to connect a sender or a receiver to the tenant.

> → Remember
>
> There are currently certain limitations when working in the Cloud Foundry environment. For more information on the limitations, see SAP Note 2752867.

The following **adapters** are available.

Adapter

Feature	Description
Mail Sender adapter	Enables SAP Cloud Integration to read e-mails from an e-mail server. To authenticate against the e-mail server, you can send the user name and password in plain text or encrypted (the latter only if the e-mail server supports this option). You can protect inbound e-mails at the transport layer with IMAPS, POP3S, and STARTTLS. The sender adapter allows you to define a schedule for polling data from the connected system. For more information on possible threats when processing e-mail content with the Mail adapter, see the product documentation.
Mail Receiver adapter	Enables SAP Cloud Integration to send e-mails to an e-mail server. To authenticate against the e-mail server, you can send the user name and password in plain text or encrypted (the latter only if the e-mail server supports this option). • You can protect outbound e-mails at the transport layer with STARTTLS or SMTPS. • You can encrypt outbound e-mails using S/MIME (supported content encryption algorithms: AES/CBC/PKCS5Padding, DESede/CBC/PKCS5Padding).
EBICS adapter	Connects an SAP Multi-Bank Connectivity corporate customer tenant to a remote receiver system that can process `Electronic Banking Internet Communication Standard` (EBICS).

Ways to Connect a Participant to the Network

There are various ways for connecting participants to the network. Each option implies a specific transport protocol. The table below outlines most frequently used integration scenarios.

Option	Supported for Type of Participant
Using the Multi-Bank Connectivity connector	Corporation

Option	Supported for Type of Participant
Using SAP NetWeaver PI on premise	Corporation Financial service provider
As SFTP client or SFTP server	Corporation Financial service provider

> **i** Note
>
> SAP Multi-Bank Connectivity is compatible with non-SAP and SAP systems. The integration of the SAP ERP systems can be accelerated through the Multi-Bank Connectivity connector.

1.1.3.2.1 Using SAP NetWeaver PI on Premise

A participant (corporation or financial service provider) can connect to SAP Multi-Bank Connectivity using an on-premise SAP NetWeaver Process Integration (PI) system (release SAP NetWeaver PI 7.1 or higher).

This connectivity option is illustrated in the following figure.

Using SAP NetWeaver PI on Premise

Using this option, the participant communicates with SAP Multi-Bank Connectivity via the XI message protocol.

The components interact with each other in the following way:

- A corporation sends messages (in business terms, a payment instruction) to SAP Multi-Bank Connectivity and receives messages (status or statement) from SAP Multi-Bank Connectivity.
- SAP Multi-Bank Connectivity forwards the messages from the corporate system to the on-premise PI system of the financial service provider and vice versa.
- The on-premise PI system (of the financial service provider) converts the payment message into a file and places the file in a folder of the financial service provider. It picks up the file and converts it into the status/statement message and forwards it to SAP Multi-Bank Connectivity.

For the payment instruction, the on-premise PI system represents the provider. For the status/statement message, the corporate system represents the provider.

This connectivity option supports secure data exchange based on public key technology (mutual authentication based on X.509 certificates).

1.1.3.2.2 Using the Multi-Bank Connectivity Connector

A corporation connects to SAP Multi-Bank Connectivity using the Connector for the SAP Multi-Bank Connectivity (Multi-Bank Connectivity connector).

> **i** Note
>
> The SAP Multi-Bank Connectivity connector is an add-on available for releases of SAP ERP 6.0 EHP 0 and higher. Within SAP S/4HANA this add-on is already embedded and can be used once a customer subscribes to SAP Multi-Bank Connectivity.

The SAP Multi-Bank Connectivity connector is integrated with the payment processing functions in SAP ERP. Following a payment run or an approval step within SAP Bank Communication Management, corporations can send the payment files automatically to financial service providers through SAP Multi-Bank Connectivity. In return, SAP ERP receives payment status reports and financial service providers' statements through SAP Multi-Bank Connectivity, and then automatically processes them.

A corporation can communicate with multiple financial service providers using a single instance of the Multi-Bank Connectivity connector, provided that these financial service providers are subscribed to SAP Multi-Bank Connectivity and the corporation has performed the required service activation with the respective financial service provider. TheSAP Multi-Bank Connectivity connector also provides a programming interface that enables corporations to further enhance the system to send and receive other message types from different business processes.

For more information on the SAP Multi-Bank Connectivity Connector, go to the help page.

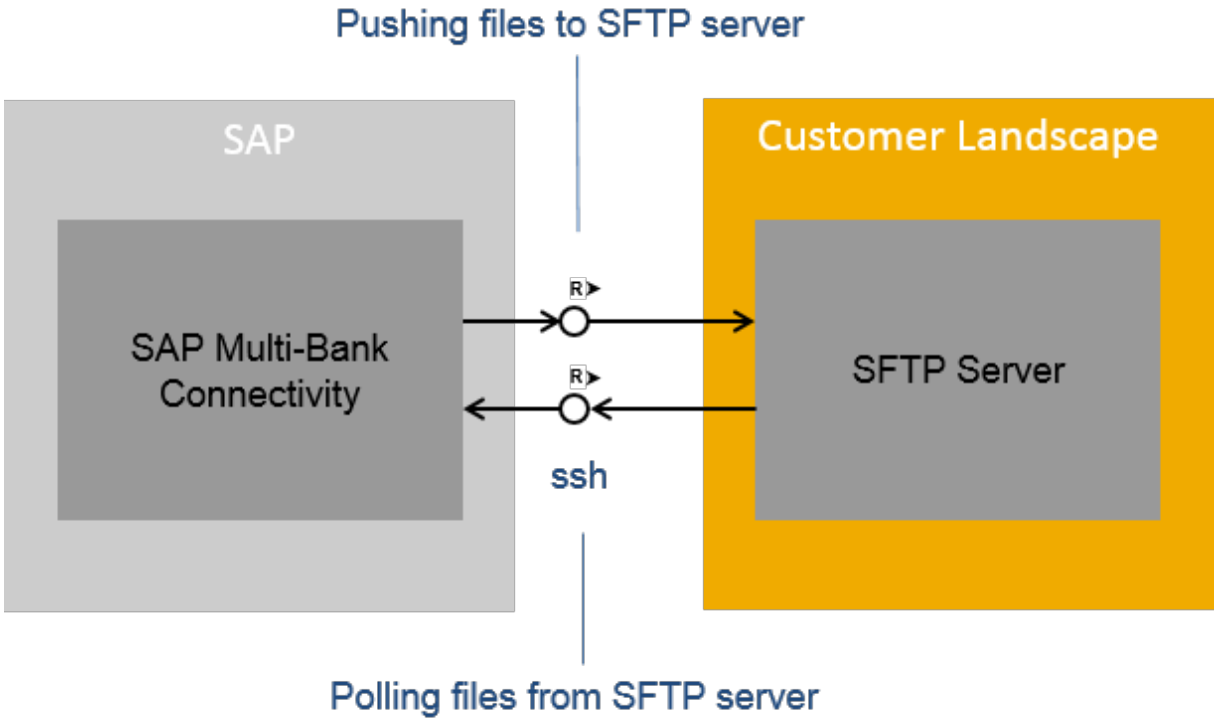
1.1.3.2.3 Using SSH File Transfer Protocol (SFTP)

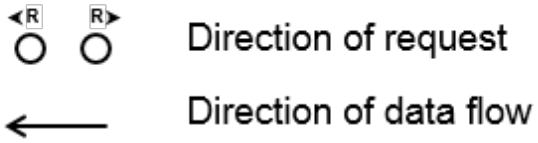
A participant (corporation or financial service provider) can connect to SAP Multi-Bank Connectivity using SSH File Transfer Protocol (SFTP).

This connectivity option requires an SFTP server to be installed within the landscape. The setup of components depends on whether the SFTP server is installed on the SAP side or within the customer landscape.

Connectivity Using an SFTP Server in the Customer Landscape

If a participant (the customer) has an SFTP server installed, it can communicate directly with SAP Multi-Bank Connectivity. The data exchange works in the following way:





- Outbound processing (from SAP Multi-Bank Connectivity to participant): SAP Multi-Bank Connectivity writes a file to a directory on the SFTP server on the participant side.
- Inbound processing (from participant to SAP Multi-Bank Connectivity): SAP Multi-Bank Connectivity periodically reads files from the SFTP server on the participant side.

1.1.3.3 Service Reliability

SAP Multi-Bank Connectivity message processing capabilities will be available with 99% uptime, running 24 hours a day, 7 days a week, and 365 days a year.

1.1.3.4 Supported Quality-of-Service

SAP Multi-Bank Connectivity supports the quality of service *At Least Once*. With this service, once SAP Multi-Bank Connectivity receives a message from a sender participant, it stores the message and sends a technical acknowledgment to the sender. It then tries to deliver the message to the receiver participant. If the receiver is not available, SAP Multi-Bank Connectivity tries again at defined time intervals until the message is sent to the receiver. If the maximum number of retries (as configured) is reached and the receiver is still not available, SAP Multi-Bank Connectivity throws an alert to the operations team. This team will act accordingly.

1.1.4 Security Information

This section provides an overview of the security-relevant aspects of SAP Multi-Bank Connectivity.

Security in SAP Multi-Bank Connectivity includes the following aspects:

- **Security aspects of the involved components of the technical system landscape**
  Scenarios based on SAP Multi-Bank Connectivity include SAP's cloud-based integration platform as well as back-end systems on the connected participant's side. Security of an SAP Multi-Bank Connectivity scenario is directly dependent on the security of the involved components.
- **Tenant isolation**
  For each participant connected to SAP Multi-Bank Connectivity, separate resources (memory, CPU, and file system) of the cloud-based integration platform are allocated – although all participants might share the same hardware. This concept is also referred to as tenant isolation.
- **Communication security**
  During the operation of an SAP Multi-Bank Connectivity scenario, the connected participants exchange data with each other based on the configured transport protocol. These protocols support different options to protect the exchanged data against unauthorized access. In addition to security at transport level, the content of the exchanged messages can also be protected by means of digital encryption and signature.
- **Data storage security**
  At several phases of the lifecycle of an SAP Multi-Bank Connectivity scenario, data is stored and, therefore, exposed to the risk of unauthorized access. There are several measures to protect stored data in SAP Multi-Bank Connectivity.
  In an error situation, dedicated experts at SAP have limited access rights to evaluate the situation. However, access to customer's business data is prevented.
- **Security aspects of the onboarding process**
  During the connection setup between a participant and SAP Multi-Bank Connectivity, data has to be exchanged between experts on the SAP and customers side. Several measures are applied to secure this data exchange.
- **High availability**
  Several measures are taken to ensure robust operation and a high level of operational performance of the SAP Multi-Bank Connectivity runtime.

1.1.4.1 Technical System Landscape

SAP Multi-Bank Connectivity is a cloud-based network that offers a single connection point across multiple services, businesses, and financial service providers. Using SAP Multi-Bank Connectivity, financial service providers can perform business processes with their corporate customers.

The underlying exchange of data is an important foundation for the provision of these services. The following figure shows the technical system landscape of SAP Multi-Bank Connectivity.

To exchange data with SAP Multi-Bank Connectivity, financial service providers and their corporate customers can choose between the following connectivity options – each supporting separate levels of security.

The chosen connectivity option determines which components come into play:

Security Aspects Related to the Technical System Landscape

Connectivity Option	Description
Using the connector for SAP Multi-Bank Connectivity	The corporate customer uses an SAP system (based on Application Server ABAP) and the Multi-Bank Connectivity connector add-on has to be installed on top of the corporate back-end system or is already available within SAP S/4HANA. Corporate customers in particular use SAP systems based on Application Server ABAP. Therefore, the corresponding Security Guide also applies to SAP Multi-Bank Connectivity.
Using SWIFT Gateway	The Society for Worldwide Interbank Financial Telecommunication (SWIFT) facilitates the secure transportation of financial messages between financial services institution and their connected partners. The SWIFT provides the platform through which payment orders/statements are issued securely. The SWIFT is partnered with an extensive list of financial institutions throughout the world and functions as a single standardized point of connection for message transmission of this type. The connection SAP Multi-Bank Connectivity has with the SWIFT, on the technical/integration level, takes the form of content collectively referred to as the *SWIFT Gateway*. Where customers have large numbers of financial institustions, the SWIFT is recommended as the most suitable integration option from a time and effort perspective.

1.1.4.2 Tenant Isolation

For each participant connected to SAP Multi-Bank Connectivity, separate resources (memory, CPU, and file system) of the cloud-based integration platform are allocated – although all participants might share the same hardware.

This concept is also referred to as *tenant isolation*.

> **i Note**
>
> A tenant represents the resources of the cloud-based integration platform of SAP Multi-Bank Connectivity allocated to a participant.

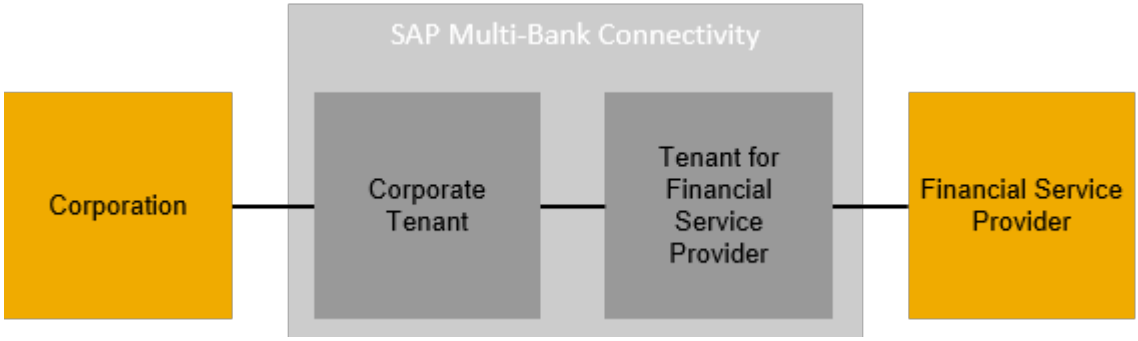
At runtime, SAP Multi-Bank Connectivity processes the data that is exchanged between the involved participants on a cluster of different virtual machines (VMs) hosted in the SAP cloud, with each VM assigned to the corresponding tenant allocated to the connected participant.

> **i Note**
>
> A virtual machine (VM) is a software implementation of a machine that executes a program like a physical machine.

SAP Multi-Bank Connectivity is designed so that it always makes sure that the involved VMs are strictly separated from each other with regard to the related participants.

In addition, each tenant uses a separate database schema, which guarantees that data of different participants is strictly separated.

The following figure illustrates this concept for the communication between a corporation and a financial service provider.



To enable a corporation to communicate with a financial service provider using SAP Multi-Bank Connectivity, tenants have to be specified for both the corporation and the financial service provider. At runtime, the corporation connects to the corporate tenant either directly through the Multi-Bank Connectivity Connector or through SFTP. The financial service provider on the other side also connects to its tenant.

The communication between the tenants within a cluster (in the example, the communication of the corporate tenant and the tenant of the financial service provider) is secured by transport level encryption (through HTTPS/SSL). If desired by the customer, encryption and digital signature based on PKCS#7 can also be applied for this communication path.

With regard to the message flow between a corporation and a financial service provider, tenant isolation comes into play in the following way: For the message flow (with payment instruction) from a corporation to a financial service provider, the corporate tenant acts as the sender tenant and the tenant of the financial service provider as the receiver tenant. Similarly, for the message flow (with payment status) from the financial service provider to the corporation, the tenant of the financial service provider acts as the sender tenant and the corporate tenant as the receiver tenant. SAP Multi-Bank Connectivity supports data isolation between these tenants by splitting the message processing step between the sender and receiver tenants.

When the sender triggers a message to the receiver, the sender tenant processes the first part of the message. Then the message is forwarded to the receiver tenant via a secure channel (based on SSL). The receiver tenant

then continues the processing. This ensures that the data of sender and receiver tenants is processed separately by its respective tenants.

1.1.4.3 Communication Security

This section provides an overview of the security features of SAP Multi-Bank Connectivity corresponding to the various types of communication and transport protocol.

The chosen transport protocol comprises options to secure the communication, as summarized in the following table.

Overview of Connectivity Options and Transport Level Security

	Protocol	Description
Using SFTP	Secure Shell File Transfer Protocol (SSH File Transfer Protocol, abbreviated to *SFTP*)	Enables you to connect an SFTP server to SAP Multi-Bank Connectivity (which acts as an SFTP client). This option is particularly useful for secure communication between SAP Multi-Bank Connectivity and non-SAP system environments. The following versions are supported: • SSH version 2 • SSH File Transfer Protocol (SFTP) version 3 or higher Supported algorithms and key length: RSA/DSA (1024)
Using SAP NetWeaver PI Using the Multi-Bank Connectivity Connector	HTTPS/SSL	Enables asynchronous HTTP/HTTPS-based WebServices communication with quality of service Best Effort. Supports SSL-based transport level security (X.509 certificate-based authentication and authorization).

On top of the chosen transport protocol, you have the option to apply additional measures to protect the exchanged data at the message level.

The following options are available:

- Encryption/decryption of message content
  Encryption allows you to encode the content of a message in such a way that only authorized parties can read it.
- Digital signing/verifying messages
  A digital signature ensures the authenticity of a message by guaranteeing the identity of the signer and that the message was not altered after signing.

Message level security based on PKCS#7/CMS Enveloped Data and Signed Data.

> **i** Note
>
> PKCS stands for *Public Key Cryptography Standards*. Digitally signing a message within Multi-Bank Connectivity is based on the CMS type Signed Data. Digitally encrypting or decrypting the content of a message is based on the CMS type Enveloped Data.

1.1.4.4 Data Storage Security

Data related to processed messages is stored for 90 days by default.

This time can be configured individually, if desired by the customer. Storage is in separate, tenant-specific database schemas, which are not shared across tenants.

1.1.4.5 Security of the Onboarding Process

To set up the connection of a new participant and SAP Multi-Bank Connectivity for the first time, experts on both the participant's and on the SAP side have to interact in a coordinated way during the onboarding process. During this process, confidential data has to be exchanged between SAP and the participant, such as server addresses or public key certificates, as well as the names of the involved persons.

To increase the security level of the SAP-participant information exchange, access to the relevant data is restricted to a small circle of experts involved in the onboarding process.

The information exchange has to take place in a coordinated way and be aligned with the configuration tasks on each side of the communication.

1.1.4.6 High Availability

To ensure that a cluster can operate reliably even if individual virtual machines crash, failover mechanisms are implemented: If a virtual machine crashes while processing a message, this incident is detected by the cluster and a new virtual machine is started automatically to take over the task of the crashed virtual machine.

Software update of the runtime environment is accomplished with a minimum downtime of about 1 minute.

1.1.5 Operating Model

An operation model clearly defines the separation of tasks between SAP and the customer during all phases of an integration project.

SAP BTP, SAP Cloud Integration (also known as Cloud Integration), and SAP Multi-Bank Connectivity have been developed on the assumption that specific processes and tasks will be the responsibility of the customer. The following table contains all processes and tasks involved in operating the aforementioned services and

specifies how the responsibilities are divided between SAP and the customer for each individual task. It does not include the operation of systems and devices residing at operational facilities owned by the customer or any other third party, as these are the customer's responsibility.

Changes to the operating model defined for the services in scope are published using the *What's New* (release notes) section of the respective product documentation on SAP Help Portal. Customers and other interested parties must review the product documentation on a regular basis. If critical changes are made to the operating model, which require action on the customer side, an explicit notification is sent by e-mail to the affected customers. If customers want to receive such notifications, they can subscribe to the relevant communication channels offered by SAP (for example, by opening a customer incident on component *LOD-HCI*).

It is not the intent of this document to supplement or modify the contractual agreement between SAP and the customer for the purchase of any of the services in scope. In the event of a conflict, the contractual agreement between SAP and the customer as set out in the Order Form, the General Terms and Conditions of SAP Cloud Services, the supplemental terms and conditions, and any resources referenced by those documents always takes precedence over this document.

Responsibilities for operating the following services are listed in the table below:

- SAP BTP (referred to as *Platform*)
- SAP Cloud Integration (briefly referred to as *Cloud Integration*)
- SAP Multi-Bank Connectivity

Responsibilities for Operating SAP BTP

		SAP Cloud Service		Responsibility	
Activity	**Task**	**Platform**	**Cloud Integration**	**SAP**	**Customer**
Communication Management	Appoint an English-speaking contact person and communicate the name to SAP. This is required to ensure timely processing of configuration change requests affecting the customer system, interacting with SAP for efficient incident processing, and other interaction between SAP and the customer.	✓	✓		✓
	Subscribe to the communication channels offered by SAP for receiving prompt information about any service disruptions, critical maintenance activities affecting the customer system, and change requests requiring action on the customer side.	✓	✓		✓
	Inform the customer about any service disruptions, critical maintenance activities affecting the customer system, and change requests requiring action on the customer side.	✓	✓	✓	

		SAP Cloud Service		Responsibility	
Activity	**Task**	**Platform**	**Cloud Integration**	**SAP**	**Customer**
Asset Management	Management of the hardware and infrastructure resources, from acquisition through disposal. This includes the request and approval process, procurement management, life-cycle management, and disposal management.	✓	✓	✓	
	Protect IT assets such as systems, network, and data from threats that arise from unauthorized physical access or physical influence on those assets.	✓	✓	✓	
Provisioning	Provisioning of resources and systems to customers in accordance with ordered package and requirements. This includes the allocation and provisioning of technical (physical and virtual) resources, such as storage, network, compute units, systems, and database hosts, the deployment of the application software and the proper initial configuration of quotas, service subscriptions, permissions, and trust configuration.	✓	✓	✓	
Integration Content Development	Design, build, deploy, and operate the integration content hosted in the application. This includes proper testing of the integration content under realistic conditions before its productive usage. Integration content may comprise integration flows, adapters, scripts, and so on.		✓		✓
Security Material Management	Create, configure, deploy, and operate (renew) security material hosted in the application. This includes proper testing of the security material under realistic conditions before its productive usage. Security material may comprise user credentials, PGP key rings, certificates, known hosts files, and so on.		✓		✓

		SAP Cloud Service		Responsibility	
Activity	Task	Platform	Cloud Integration	SAP	Customer
	Create, configure, deploy, and operate the keystore artifact hosted in the application. This includes the import of public and private keys used for certificate-based authentication when sending a message from the application.		✓		
Message Transmission	Correct transmission of the messages within the according constraints offered by the application. SAP makes no warranty and shall have no liability for the contents of any message transmitted via the application, including the accuracy or completeness of any information contained in a message.		✓	✓	
Change Management	Apply regular product increments, as well as corrections to the application to avoid incidents with minimal possible disruption of normal operations. Ensure that all changes (such as changes in scheduling of administrative jobs, enabling the product capabilities, and so on) are evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed prior to implementation.		✓	✓	
	Perform upgrades of the application in a monthly cycle. Emergency changes, for example, triggered by Incident Management processes, have accelerated testing, approval, and implementation.		✓	✓	
	Apply regular product increments, as well as corrections to the infrastructure, systems, and services to avoid incidents with minimal possible disruption of normal operations. Ensure that all changes (such as updates of the Java runtime, operating system patches, and so on) are evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed prior to implementation.	✓		✓	

		SAP Cloud Service		Responsibility	
Activity	Task	Platform	Cloud Integration	SAP	Customer
	Perform upgrades of the infrastructure, systems, and services in a bi-weekly cycle. Emergency changes, for example, triggered by Incident Management processes, have accelerated testing, approval, and implementation.	✓		✓	
	Consume latest version of provisioned infrastructure, systems, and services (for example, Java runtime, operating system) to run the application in the customer account.	✓	✓	✓	
	Collaborate with SAP to ensure timely processing of change requests affecting the resources in the customer account.	✓	✓		✓
	Prompt delivery of patches for security vulnerabilities in the operating system and database hosted by the application. This includes reviewing the priority of the relevant patches, assessing the risk, and finally implementing the patch via the Change Management process.	✓	✓	✓	
Incident Management	Process incidents reported by the customer according to the Service Level Agreement. The incident is recorded and prioritized in the incident tracking system (BCP). Monitor the status and progress of the incident throughout its whole lifecycle and give regular status updates to the customer.	✓	✓	✓	
	In the event of incidents, make reasonable effort to support end users and manage their incidents, to explore self-help tools to find already documented solutions, and to liaise with SAP support in the event of new problems to ensure timely processing of incidents affecting the resources in the customer account.	✓	✓		✓
	Confirm incident resolution in the incident tracking system (BCP).	✓	✓		✓

		SAP Cloud Service		Responsibility	
Activity	**Task**	**Platform**	**Cloud Integration**	**SAP**	**Customer**
Service Requests	Process service requests reported by the customer according to the Service Level Agreement. The service request is recorded and prioritized in the service request tracking system (BCP). Monitor the status and progress of the service request throughout its whole lifecycle and give regular status updates to the customer.	✓	✓	✓	
	Confirm service request completion in the service request tracking system (BCP).	✓	✓		✓
Backup & Restore	Perform a backup of the database systems hosted in the customer account. A database log backup is done every 10 minutes and stored on the primary storage. Every 2 hours the logs are transferred from primary to secondary storage. Full data backup is done every day.	✓	✓	✓	
	Restore previously backed-up data to recover to a consistent state. Verify the completeness of the restored data based on log files created during the recovery and smoke tests to verify the system's consistency.	✓	✓	✓	
	Give regular status updates to the customer throughout the entire restore procedure.	✓	✓	✓	
	Collaborate with SAP to ensure timely processing of data restores if required.	✓	✓		✓
	Validate logical integrity and consistency of the restored data.	✓	✓		✓
User Access Management	Provide a proper user to SAP, to which the Account Administrator role for the customer account is to be granted by SAP as part of the provisioning process.		✓		✓
	Grant the Administrator role for the customer account to the user nominated by the customer.		✓	✓	

		SAP Cloud Service		Responsibility	
Activity	Task	Platform	Cloud Integration	SAP	Customer
	Manage users, permissions, and security configurations within the customer account.	✓	✓		✓
System Monitoring	Ensure availability of the customer system according to the Service Level Agreements as agreed in the contractual agreement between SAP and the customer, by active monitoring, prompt issue detection, and incident prevention.	✓	✓	✓	
	Monitor the resource consumption (memory, CPU, storage) to detect issues in technical operations.	✓	✓	✓	
Malware Management	Ensure that the infrastructure and platform services are free of viruses, spam, spyware, and other malicious software. If malware is detected, an auto-notification is generated, which is assessed and resolved by the operator.	✓	✓	✓	
Application Management	Design, develop, deploy, configure, maintain, and operate the application within the customer account. This includes maintaining a staged environment for application delivery (if required), application resource management, and managing application availability and performance.	✓			✓
	Provide infrastructure, tools, and application programming interfaces for the lifecycle management and operations of the application in the customer account.	✓			✓
	Regularly adopt the latest versions of the tools for lifecycle management and operations offered at the SAP Development Tools site.	✓			✓
Network Management	Manage the network isolation of the accounts provisioned to the customer.	✓	✓	✓	

		SAP Cloud Service		Responsibility	
Activity	Task	Platform	Cloud Integration	SAP	Customer
	Operate the network infrastructure transparently for customers, ensuring elasticity, high availability, and security.	✓	✓	✓	
	Create and manage own Web domain for the application in the customer account to ensure data isolation.	✓			✓
Penetration Testing	Inform SAP about any penetration testing that shall be performed for the customer system and ask for their approval. Testing is not allowed on any systems or resources shared with other customers. The results, if any, from the test are to be treated strictly as the confidential information of SAP and the customer and are not to be shared with any person or entity without explicit written authorization from SAP. Customers are required to share the results with SAP and work together with SAP operations to mitigate or remedy any security issues.	✓	✓		✓
Decommissioning	Ensure the secure deletion of data and/or hardware disposal. This includes the disassembling of systems along with peripherals and their removal. Before dismantling and handover for further use or return to the vendor, the data is wiped securely from the system.	✓	✓	✓	
	Request a final export of customer data from the application within the time stated in the Terms & Conditions document. The export of customer data can be requested by opening a BCP incident on component *LOD-HCI**.				✓

		SAP Cloud Service		Responsibility	
Activity	Task	Platform	Cloud Integration	SAP	Customer
	Perform a final export of the customer data from the service using the provided data export self services within the time stated in the Terms & Conditions document. The following services are provided: • Export of Message content stored through persist flow-step in an integration flow by means of an API • Export of Customer data in JMS queues • Export of Integration Content • Export of Security Key Material only for public keys		✓		✓

1.1.6 Support Information

If you require any support or have queries, you can contact SAP:

- SAP Multi-Bank Connectivity telephone numbers for support (24x7) on SAP Support Launchpad
- 24x7 via incident report to be created on the component *LOD-FSN* at http://support.sap.com
- To receive availability notfications, sign up at Cloud System Notification Subscriptions

1.1.7 Onboarding and Service Activation

Two kinds of process are relevant when starting operating scenarios based on SAP Multi-Bank Connectivity:

- **Onboarding:** This is the process of connecting a participant (either a financial service provider or a corporation) to SAPMulti-Bank Connectivity. Onboarding covers all tasks that are necessary in order to configure the data exchange and the connection between the corporation's or financial service provider's system and SAP Multi-Bank Connectivity.
  A customer is onboarded to both a test and a production landscape.
  Before a financial service provider can start collaborating with a corporate customer based on SAP Multi-Bank Connectivity, the financial services provider and the corporate customer both have to be connected to Multi-Bank Connectivity. In other words, onboarding is a one-time activity that is a prerequisite for service activation.
- **Service activation:** This is the process when a financial service provider starts collaboration with a corporate customer. On request, SAP activates the connection between the two participants and informs

them once the connection is complete. This allows the newly connected participants to carry out message flow testing across the service prior to moving into the production landscape.
A customer service activation is carried out in both a test and a production landscape.

1.1.7.1 Use Cases

There are different onboarding use cases depending on the kind of participant (bank or corporation) and on the chosen connectivity between participant and SAP Multi-Bank Connectivity. Depending on the use case, the details of some steps of the onboarding process vary.

The following basic use cases are supported:

Overview of Onboarding Use Cases

Use Case	System Landscape
SFTP server@bank	An SFTP server is hosted by the bank, and the SAP Multi-Bank Connectivity bank tenant acts as SFTP client.
SFTP server@SAP	An SFTP server is hosted by SAP, and both the SAP Multi-Bank Connectivity bank tenant and the bank system act as SFTP client.
SFTP server@Bank and @SAP (*hybrid use case*)	This use case is a combination of the first two use cases.
Other communication protocol like AS2, SOAP or REST	Other communication protocols can be used to establish a connection between a bank and SAP Multi-Bank Connectivity.
Corporation using the Multi-Bank Connectivity Connector	A corporate SAP system connects to SAP Multi-Bank Connectivity using the Multi-Bank Connectivity connector.
Corporation using SWIFT via SAP Multi-Bank Connectivity	A corporate customer connects via SAP Multi-Bank Connectivity to SWIFT.

> **i Note**
>
> SFTP polling is supported in the following way: the same file can be polled by multiple endpoints configured to use the SFTP channel.

On top of the basic use cases, additional use cases that depend on the following aspects:

- Applied message level security
- Implementing the pull communication pattern
  Using this pattern, messages received by a sender participant are stored in a tenant-specific data store at SAP Multi-Bank Connectivity. The receiver participant then polls (reads) the message from there. This pattern *shifts the control* of message processing to the participant. That way, failure situations due to unattainability of a receiver can be prevented.

Related Information

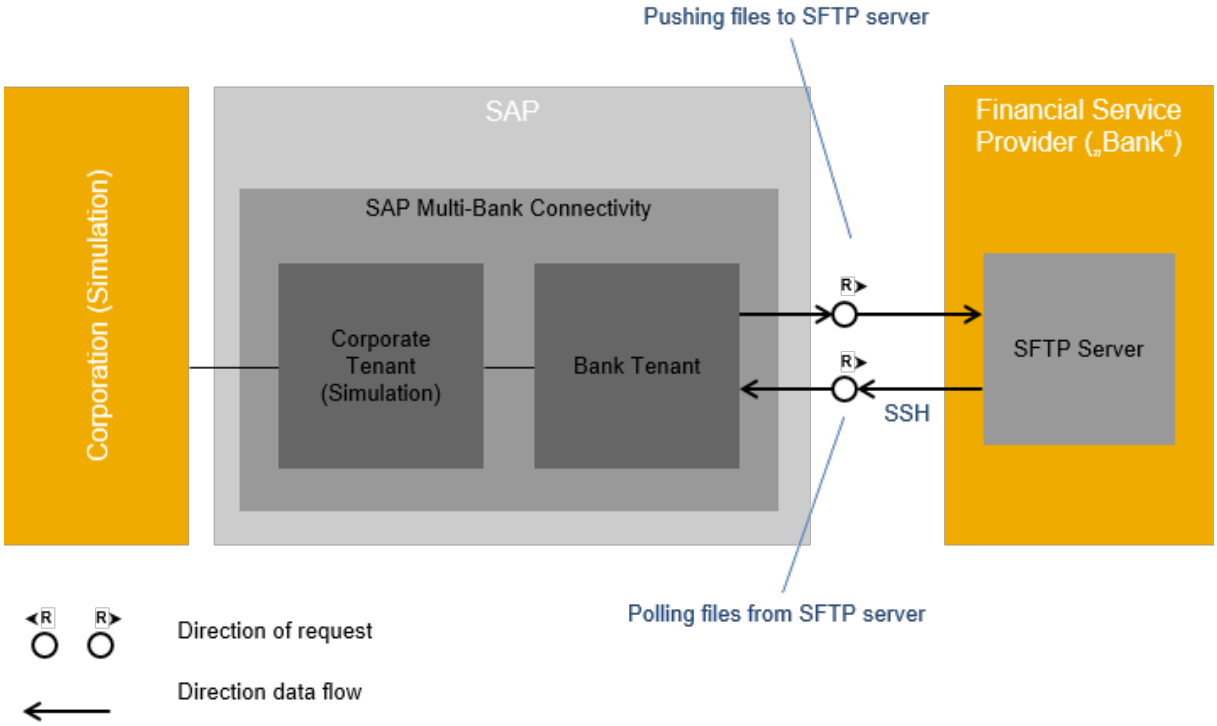
SFTP Server@Bank [page 27]

SFTP Server@SAP [page 29]
SFTP Server@SAP and SFTP Server@Bank (Hybrid Use Case) [page 31]
Other Communication Protocols like AS2, SOAP or REST [page 33]
Security Artifact Exchange [page 33]
Corporation Using SWIFT via SAP Multi-Bank Connectivity [page 36]

1.1.7.1.1 SFTP Server@Bank

You can set up SFTP-based communication between a bank and SAP Multi-Bank Connectivity with an SFTP server hosted by the bank. This topic explains the setup of components and summarizes the keys that need to be exchanged during onboarding.

The following figure illustrates the system landscape.

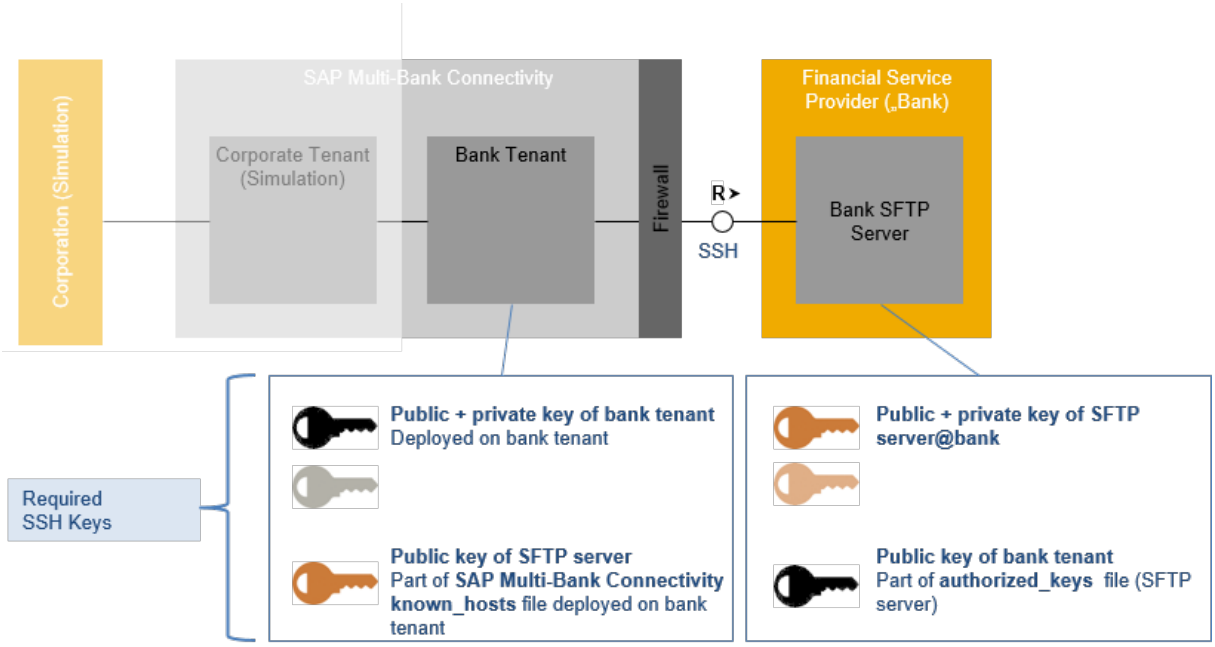


The message sent to the bank from the simulated corporation is processed first by the SAP Multi-Bank Connectivity corporate tenant (simulation) and handed over from there to the bank tenant. The bank tenant (as SFTP client) writes the SFTP message to the SFTP server on the bank side.

For the data flow in the other direction, SAP Multi-Bank Connectivity (bank tenant) as SFTP client picks up (pulls) the data from the SFTP server and forwards the data to the corporate tenant (simulation).

For productive operation, the corporate tenant (simulation) is replaced by the productive corporate tenant and the simulated corporate system by the productive one.

The following figure shows the overview of the required keys on the SAP side and on the bank side.



To ensure secure data transfer between the components, asymmetric SSH key pairs are used to encrypt and decrypt the symmetric keys that are actually used to secure the data transfer session between two components (session keys).

The following table summarizes how the different keys are related to each other and what role they play in the secure SSH connection process.

> **i Note**
>
> Note that separate key sets are used for test and for productive usage. Therefore, the components *bank tenant* and *bank SFTP server* in the figure stand for either test or productive bank tenant and bank SFTP server (both connected to the same simulated corporate tenant during bank onboarding).

Required SSH Keys

Keystore	Key	Description
Bank tenant keystore Required for communication with the bank client. Deployed on the bank tenant.	Private SSH key of SAP Multi-Bank Connectivity bank tenant	Generated by SAP (and remains in keystore).
	Public SSH key of SAP Multi-Bank Connectivity bank tenant	Generated by SAP and handed over to the bank. The bank stores this key in the *authorized_keys* file on the SFTP server.
Bank keystore Required for communication with SAP Multi-Bank Connectivity (bank tenant).	Private SSH key of SFTP server@bank	Generated by the bank (and remains in keystore).
	Public SSH key of SFTP server@bank	Generated on the bank side and handed over to SAP. SAP stores this public key in the *known_hosts* file related to the bank tenant and deploys it on the bank tenant.

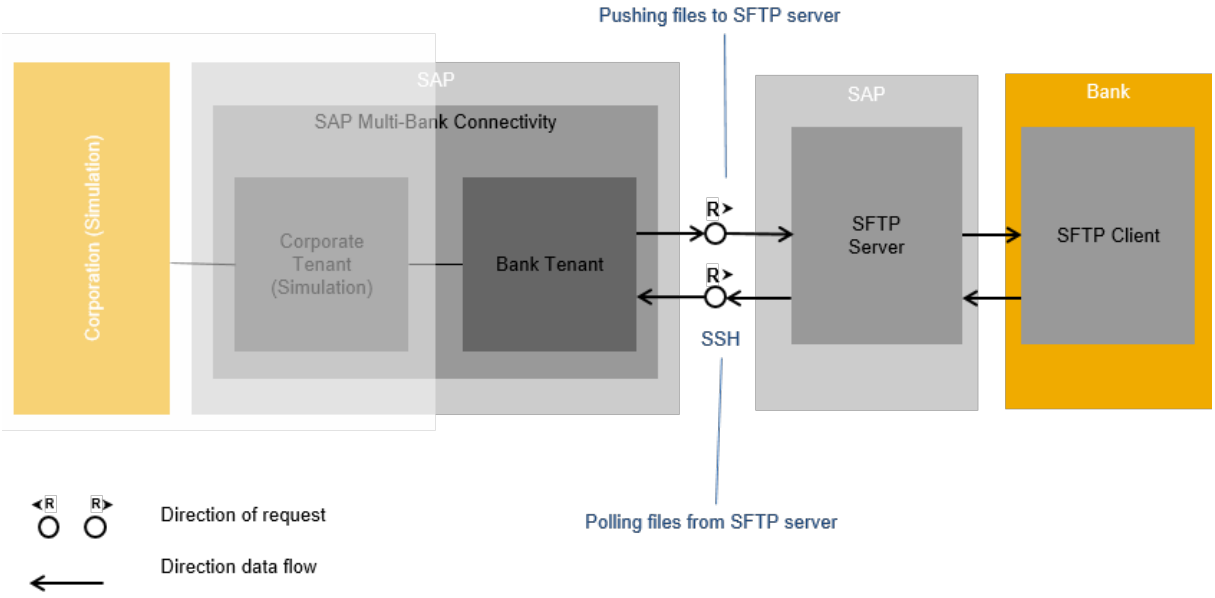
To implement this setup, the required key pairs have to be generated on each side of the communication and the public keys have to be exchanged with the corresponding counterpart.

To keep an overview of all required and exchanged keys during onboarding and productive operation, we recommend that you adhere to specific key-naming conventions.

1.1.7.1.2 SFTP Server@SAP

You can set up SFTP-based communication between a bank and SAP Multi-Bank Connectivity with an SFTP server hosted at SAP. This topic explains the setup of components and summarizes the keys that need to be exchanged during onboarding.

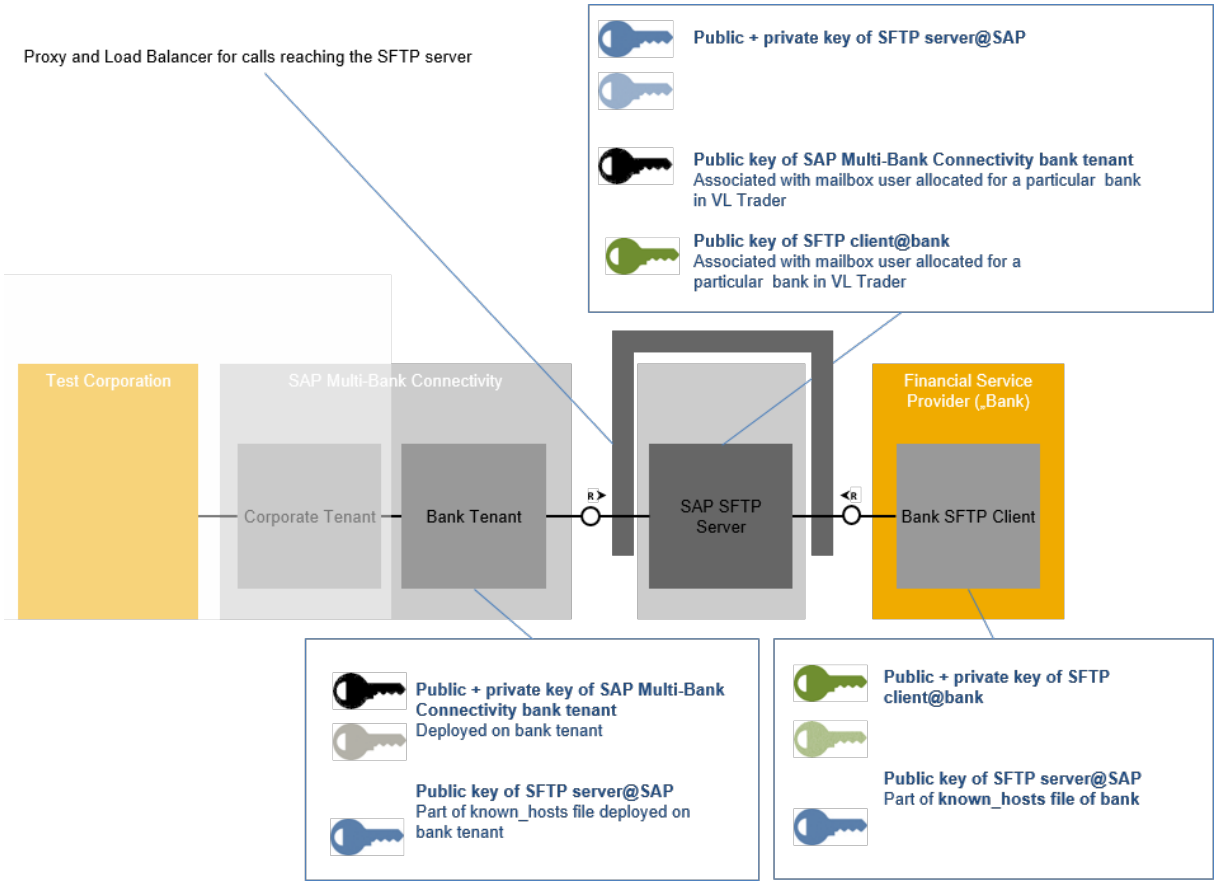
The following figure illustrates the system landscape.



The bank tenant as SFTP client writes a payment message to the SFTP server. The bank sends an acknowledgment message to the SFTP server (to a bank-specific inbox). In the other direction, the bank tenant as SFTP client picks up the message from the SFTP server from a bank-specific inbox.

To ensure secure data transfer between the components, asymmetric SSH key pairs are used to encrypt and decrypt the symmetric keys that are actually used to secure the data transfer session between two components (session keys).

The following figure shows the involved components and indicates the required SSH keys.



In this setup, both SAP Multi-Bank Connectivity and the bank system act as SFTP clients when writing (pushing) or reading (pulling) files to or from the SFTP server. A proxy and a load balancer are interconnected between the bank tenant or SFTP client@bank and the SFTP server@SAP for calls reaching the SFTP server@SAP.

Note that no keys need to be deployed on the load balancer. The required keys are forwarded from the SFTP server. The following table summarizes the different required keys and indicates what role they play in the secure SSH connection process.

> **i Note**
>
> Note that separate key sets are used for test and for productive usage.

Required SSH Keys

Key	Description
Private key of SAP Multi-Bank Connectivity bank tenant	Generated by SAP (and remains there).
Public key of SAP Multi-Bank Connectivity bank tenant	Associated with the SAP Multi-Bank Connectivity mailbox user allocated for a particular bank (tenant) on the SFTP server@SAP.
Private key of SFTP server@SAP	Generated by SAP (and remains there).

Key	Description
Public key of SFTP server@SAP	The bank stores this public key in a known_hosts file. SAP Multi-Bank Connectivity stores this public key in the known_hosts file and deploys it on the bank tenant.
Private key of SFTP client@bank	Generated on the bank side (and remains there).
Public key of SFTP client@bank	Associated with the bank mailbox user allocated for the bank on the SFTP server@SAP.

To implement this setup, the required key pairs have to be generated on each side of the communication and the public keys have to be exchanged with the corresponding counterpart, as illustrated in the figure and table above.

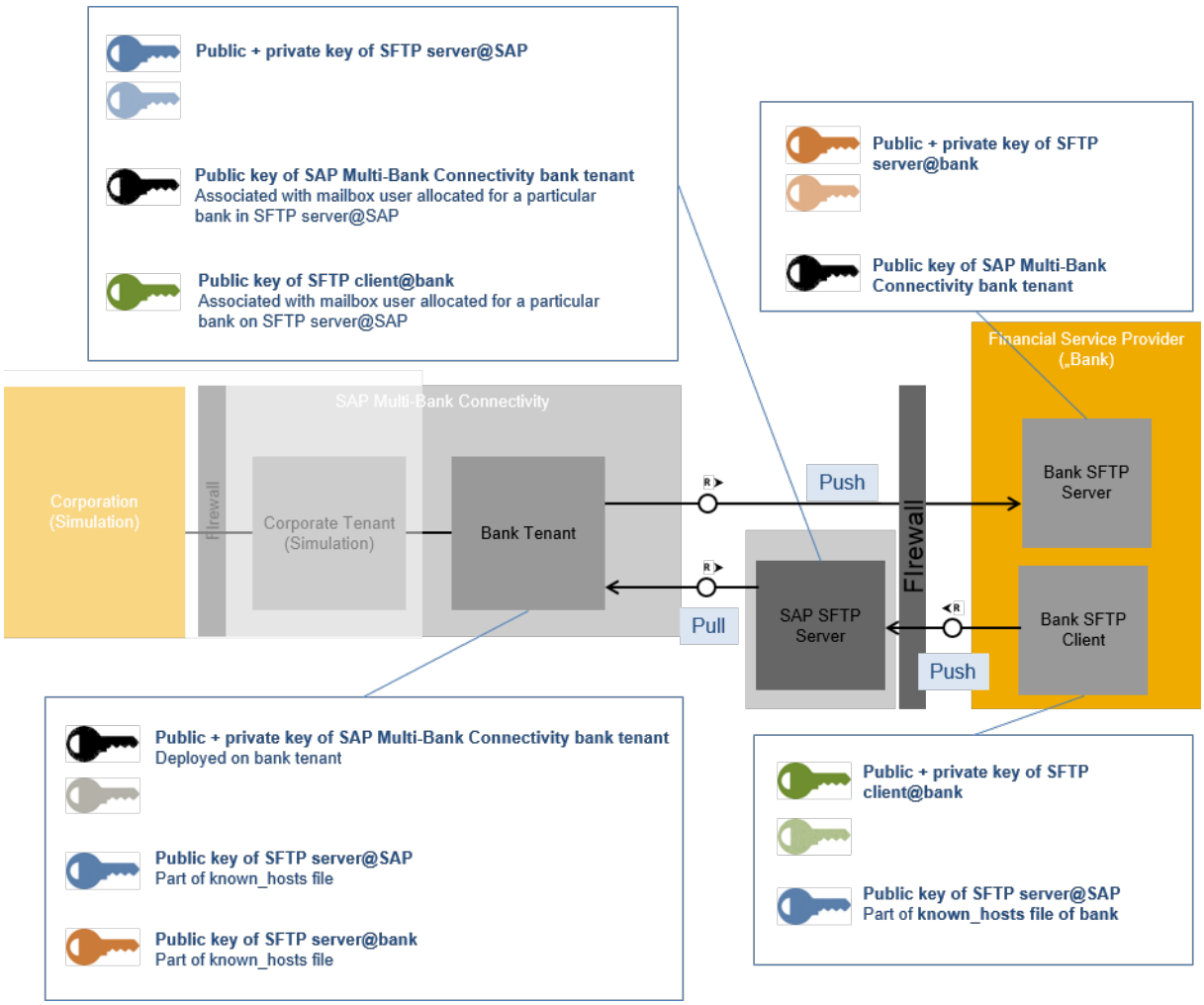
To keep an overview of all required and exchanged keys during onboarding and productive operation, we recommend that you adhere to specific key-naming conventions.

1.1.7.1.3 SFTP Server@SAP and SFTP Server@Bank (Hybrid Use Case)

You can set up SFTP-based communication between a bank and SAP Multi-Bank Connectivity with SFTP servers hosted both at SAP and on the bank side. This topic explains the setup of components and summarizes the keys that need to be exchanged during onboarding.

For the SFTP server@SAP the same concepts apply as for the use case SFTP Server at SAP.

The following figure shows the involved components and indicates the required SSH keys.



In this use case, the SAP Multi-Bank Connectivity runtime (bank tenant) acts as SFTP client in the following cases:

- When pushing files to the SFTP server@bank
- When pulling files from the SFTP server@SAP

The SFTP client@bank also acts as SFTP client when pushing files to the SFTP server@SAP.

As this use case is a combination of the use cases SFTP server@SAP and SFTP server@bank, additional keys are required and need to be exchanged during onboarding. However, for the individual keys the same applies as already described for the two other use cases. Therefore, refer to the corresponding sections. In summary, note the following:

- The SAP Multi-Bank Connectivity runtime (bank tenant) is connected to the SFTP server@bank. Therefore, the public key of the bank tenant is required to configure the SFTP server@bank and the public key of the SFTP server@bank is required to configure the SAP Multi-Bank Connectivity runtime.
- The SAP Multi-Bank Connectivity runtime (bank tenant) is connected to the SFTP server@SAP. Therefore, the public key of the bank tenant is required to configure the SFTP server@SAP and the public key of the SFTP server@SAP is required to configure the SAP Multi-Bank Connectivity runtime.
- The SFTP server@SAP is connected to the SFTP client@bank. Therefore, the public key of the SFTP client@bank is required to configure the SFTP server@SAP and the public key of the SFTP server@SAP is required to configure the SFTP client@bank.

1.1.7.1.4 Other Communication Protocols like AS2, SOAP or REST

There are other protocols available, such as, AS2, SOAP to connect to SAP Multi-Bank Connectivity.

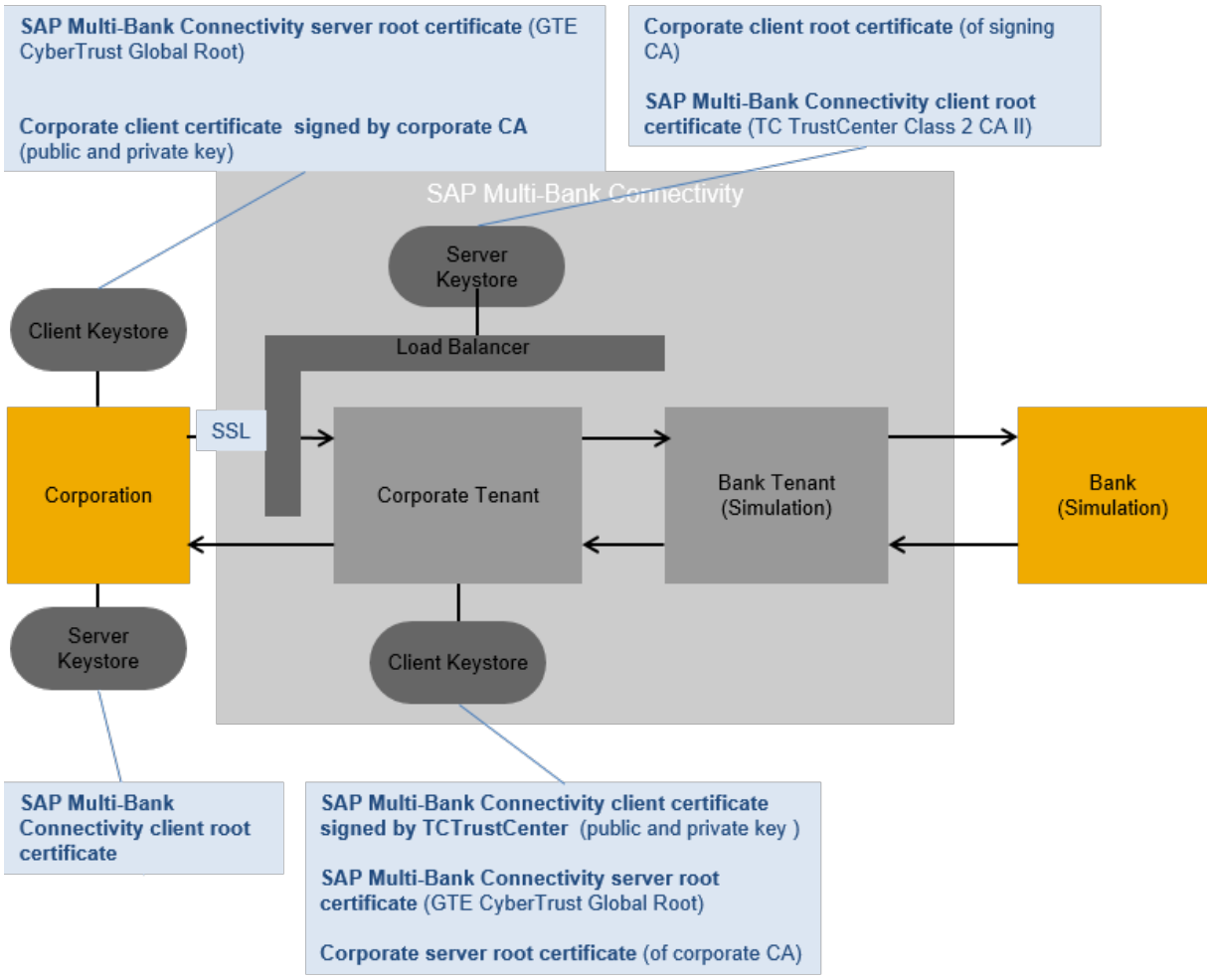
These scenarios are typically used by financial institutions and require customer-specific discussions during onboarding and service activation. Based on the protocols supported, SAP and the financial institutions need to discuss available protocols and security details for various processes.

1.1.7.1.5 Security Artifact Exchange

This section summarizes the concepts that are used when setting up connectivity between a corporation (using the connector for SAP Multi-Bank Connectivity) and SAP Multi-Bank Connectivity.

Required Keystores and Public Key Certificates

Transport level security HTTPS/SSL is based on X.509 certificates. The following figure shows the required keystores and certificates for the communication from the corporation to the corporate tenant.



In total, the following keystores are required to set up SSL-based communication between a corporate system and SAP Multi-Bank Connectivity.

Keystore	Certificate/Key	Required By	Description
SAP Multi-Bank Connectivity client keystore (`keystore.jks` file) Has to be deployed on the corporate tenant.	SAP Multi-Bank Connectivity client certificate (public and private key) signed by CA	SAP	Contains the public and private keys required to authenticate SAP Multi-Bank Connectivity as the sender of messages (for messages sent from SAP Multi-Bank Connectivity to a corporate back-end system or to a bank tenant). The client certificate is generated by SAP and then signed by a certification authority (CA). **i Note** For SSL-based communication, a separate private key should be used for each corporation. As it is only possible to deploy the complete keystore (containing the private and public key), a separate keystore has to be created for each corporation.
	Corporate server root certificate (certificate of issuer of corporate certificate)	SAP	Required to authenticate the corporate system as the receiver of messages. This certificate has to be imported into the SAP Multi-Bank Connectivity client keystore.
SAP Multi-Bank Connectivity server keystore	Corporate client root certificate	SAP	Required to authenticate the corporate system when sending messages sent to the corporate tenant. This certificate needs to be imported into the SAP Multi-Bank Connectivity server keystore.

Keystore	Certificate/Key	Required By	Description
	SAP Multi-Bank Connectivity client root certificate	SAP	Required for the following: • To authenticate the bank tenant as the sender of messages (inbound messages sent from the bank tenant to the corporate tenant) • To authenticate the corporate tenant as the sender of messages (inbound messages sent from the corporate tenant to the bank tenant)
Corporate client keystore Configured using the Trust Manager (transaction *STRUST*)	Corporate client certificate (public and private key part)	Corporation	Required to authenticate the corporate system as the sender of messages.
	SAP Multi-Bank Connectivity server root certificate (certificate of issuer of SAP Multi-Bank Connectivity server certificate)	Corporation	Required to authenticate SAP Multi-Bank Connectivity as the receiver of messages. The load balancer handles inbound message processing with regard to SAP HANA Cloud. SAP has to hand over this root certificate to the corporation (of the sending corporate system). This certificate has to be imported into the client keystore (PSE).
Corporate server keystore Configured using the Trust Manager (transaction *STRUST*)	SAP Multi-Bank Connectivity client root certificate (certificate of issuer of SAP Multi-Bank Connectivity client certificate)	Corporation	Required to authenticate SAP Multi-Bank Connectivity as the sender of messages.

In addition to the certificates illustrated in the figure and summarized in the table, the SAP Multi-Bank Connectivity client certificate is required to configure the user mapping in the corporate back-end system. This mapping is required because messages from SAP Multi-Bank Connectivity have to run under a technical user and therefore have to be mapped prior to being processed in the corporate back-end system.

To keep an overview of all required and exchanged keys during onboarding and productive operation, we recommend that you adhere to specific key-naming conventions.

1.1.7.1.6 Corporation Using SWIFT via SAP Multi-Bank Connectivity

This section summarizes the concepts that are used when setting up connectivity from SAP Multi-Bank Connectivity to SWIFT for a specific corporation.

Use

To establish the connection with SWIFT, SAP operates SWIFT software, SWIFT-specific hardware and hosts leased lines to SWIFT.

This setup leverages the connection between the corporate customer (SAP ERP system) and SAP Multi-Bank Connectivity using the SAP Multi-Bank Connectivity Connector. In addition, SWIFT parameters have been added via configuration in the SAP Multi-Bank Connectivity Connector. These parameters are mapped to the extended header of the web service to SAP Multi-Bank Connectivity.

Within SAP Multi-Bank Connectivity, the respective XMLv2 file is generated and message digest is calculated. Afterwards the message is passed to the SWIFT infrastructure. SAP supports FIN and FileAct based communication.

On the way back from SWIFT to the corporate customer, SAP Multi-Bank Connectivity receives the messages from SWIFT in a defined folder structure and forwards these messages without the XMLv2 envelop and after validating the message signature to the SAP Multi-Bank Connectivity Connector in the respective SAP ERP system. Acknowledgments are mapped to an ISO 20022 PAIN.002 format before they get forwarded to the ERP system.

1.2 What's New

See the roadmap for what is new in SAP Multi-Bank Connectivity.

1.2.1 Release 2020 Q4

These release notes correspond to the customer shipment in **2020 Q4**.

New Features

- Request intraday or end-of-day bank statement from SAP ERP or S/4HANA system
  For more information, see the feature Initiation of ad-hoc bank account (intraday) statement requests in SAP Road Map Explorer.

- Integration with payroll processes in SAP SuccessFactors
  For more information, see the feature Tighter integration with solutions for payroll processes in SAP Road Map Explorer.

1.2.2 Release 2020 Q2

These release notes correspond to the customer shipment in **2020 Q2**.

New Features

- Integration with SAP S/4HANA Finance for advanced payment management
  For more information, see the feature Optimize payment processing using a cloud solution for centralized payments in SAP Road Map Explorer.

1.2.3 Release 2019 Q4

These release notes correspond to the customer shipment in **2019 Q4**.

New Features

- Automation of MT300/320 messages in combination with SAP Treasury and Risk Management
  For more information, see the feature Treasury and Risk Management - Correspondence Integration with SWIFT Network in SAP Road Map Explorer.
- Translation of SWIFT DLV/ACK/NAK to PAIN.002 in order to enable automated processing
- Enablement of MBC status messages for confirming receipts and processing of messages
- Automation of bank fee reports (CAMT.086)
- Enablement of EBICS approvers passed from SAP ERP system
- Translation of EBICS HAC messages to PAIN.002 in order to enable automated processing
- Unzipping of files from banks in SAP ERP or S/4HANA system

1.2.4 Release 2018-09-28

These release notes correspond to the customer shipment on **2018-09-28**.

New Features

- Integration with EBICS
  Enables customers of SAP Multi-Bank Connectivity to be connected to their banks using EBICS.

1.2.5 Release 2018-02-28

These release notes correspond to the customer shipment on **2018-02-28**.

New features

Title	Description
SAP Financial Services Network renamed	SAP Financial Services Network has been renamed to SAP Multi-Bank Connectivity.
Integration with SWIFT	SAP Multi-Bank Connectivity is integrated with SWIFT. You can now transfer messages using SWIFT.

1.2.6 Release 2015-11-21

These release notes correspond to the customer shipment on **2015-11-21**.

New features

Title	Description
Open PGP: verification of uncompressed data packets	For input messages (received by SAP FSN) to be verified using Open PGP, the Compressed Data packet is now optional (it has been mandatory before this release).

1.2.7 Release 2015-08-01

These release notes correspond to the customer shipment on **2015-08-01**.

New features

Title	Description
Accessing payment batches based on company code	Buisness users at a corporation can view or approve the payment bactches specific to their company code(s)

1.3 SAP Multi-Bank Connectivity Security Datasheet

SAP Multi-Bank Connectivity (Multi-Bank Connectivity) is an on-demand solution that connects financial institutions and other financial service providers with their corporate customers on a secure network owned and managed by SAP. The network offers multiple services in one single channel while supporting the deployment of new services. As key benefits, the solution simplifies connectivity, automates financial transactions, reduces payment rejection rates, eases reconciliation, and provides enhanced visibility to corporate treasury. In order to fulfill the stringent security requirements of the financial industry, Multi-Bank Connectivity implements comprehensive security measures in the area of physical security, software security, and information security.

This document provides a concise summary of these measures. The reader is expected to have a basic understanding of IT security.

For more details, see the additional information available on Multi-Bank Connectivity.

Terminology

For simplicity, financial service providers are referred to as *banks*.

When interacting with Multi-Bank Connectivity, corporate customers send payment instructions to Multi-Bank Connectivity; banks send transaction status information and account reports. This document uses the term *Multi-Bank Connectivity message* to refer to all these types of data. If reference is made to a specific type of Multi-Bank Connectivity message, the specific term is used, for example, payment instruction.

1.3.1 The Multi-Bank Connectivity Cloud Scenario

1.3.1.1 Outsourced Community Cloud Scenario

According to *NIST Cloud Computing Synopsis and Recommendations (special publication 800-146)*, Multi-Bank Connectivity can be regarded as an *Outsourced Community Cloud*. Here the term *outsourced* means outsourced from the Multi-Bank Connectivity customer perspective. In this scenario, SAP hosts the Multi-Bank Connectivity service as a cloud solution. The Multi-Bank Connectivity cloud solution is targeted at and can be accessed only by a specific community consisting of corporate customers and financial institutions. The members of this community have the same use cases and have similar security and compliance requirements.

1.3.1.2 SaaS Provider/Consumer Scope of Control

According to the list of cloud provider/cloud consumer *scope of control models* in *NIST Cloud Computing Synopsis and Recommendations (special publication 800-146)*, Multi-Bank Connectivity belongs to the category *SaaS Provider/Consumer Scope of Control* (where *SaaS* means *Software-as-a-Service*).

Provider Control

In the *SaaS Provider/Consumer Scope of Control* model, SAP (the provider) has administrative control over the application and has total control over middleware, operating system, and hardware.

	SAP
Control over	
Application	Administrative control
Middleware	Total control
Operating System	Total control
Hardware	Total control

1.3.1.3 Push/Pull Model

Customers connect to Multi-Bank Connectivity in such a way that they are always the initiating party of an Multi-Bank Connectivity message.

This is referred to as the *push/pull model*. In this model, the customer pushes data to Multi-Bank Connectivity and pulls data from Multi-Bank Connectivity. The advantage in terms of security is that the customer can keep its existing network perimeter (firewall) configuration because Multi-Bank Connectivity does not call into the customer's landscape. Multi-Bank Connectivity also supports other models such as the push/push model, in which the customer has to open the firewall.

1.3.1.4 Global Distribution

Multi-Bank Connectivity is offered by the SAP data center in St. Leon-Rot, Germany. An additional data center is located in the US, in Ashburn, VA. This additional data center is used as a secondary site for disaster recovery.

Details of Data Centers

Data Center	Address	Tier Level	SAP-Owned Data Center/ Third-Party Data Center	SAP-Operated	Certifications driven by solutions running in this data center, or by the data center itself	Multi-Bank Connectivity Use
St. Leon-Rot, Germany	c/o SAP AG, SAP-Allee, Geb. 16, 68789 St. Leon-Rot, Germany	IV	SAP-owned data center	n/a	ISO27001 ISO22301 SSAE 16	Primary data center for hosting customers
US, Ashburn, VA	c/o Verizon Business - IAD6, 21830 UUNET WAY, Ashburn, VA 20147, USA	III/III+	Third-party data center	yes	SSAE16-SOC2	Secondary data center for hosting customers

> **i** Note
>
> **SAP-operated** means that Multi-Bank Connectivity is a colocation tenant in a non-SAP owned facility. The facility itself offers physical security, power, ping and pipe, but nothing in the SAP cage. Multi-Bank Connectivity uses a floor-to-roof caged space in which all the equipment is owned, installed, and operated by SAP.

1.3.2 Technical Security

Technical security covers all security-related aspects of how data is protected by the framework during the execution of an Multi-Bank Connectivity scenario, for example, how messages are protected by encryption and digital signatures, or how data is securely stored during the lifetime of a scenario.

1.3.2.1 Identity Management and Permissions

In the Multi-Bank Connectivity cloud, incoming Multi-Bank Connectivity messages are authenticated by the load balancer, which checks the received client certificate against the configured list of trusted CAs (CA=certificate authority).

Dialog users are authenticated against the SAP ID (Identity) Service. The SAP ID Service is the central service for the process of managing identities and their life cycles. Mainly, SAML-based authentication is used within Multi-Bank Connectivity for the authentication of dialog users. Selective internal operational access is secured by basic authentication. Multi-Bank Connectivity uses the SAP ID Service Enterprise Password Policy. This password policy is the strictest one offered by the SAP ID Service and restricts the number of previously used passwords, the maximum password age, and the maximum length of time a password can be unused.

Access to all functions, whether invoked manually by dialog users or automatically (for example, by a scheduler), is protected by a permission check. Multi-Bank Connectivity maintains a fine-grained permission

concept. Fine-grained permissions are grouped and assigned to different personas such an SaaS administrator (Software-as-Service administrator) or tenant administrator. All permission assignments are tenant-specific, except for the SaaS administrator, who has broader permissions.

For outbound communication, the receiver system is responsible for providing authentication, authorization, and the related identity management services.

1.3.2.2 Data Storage and Location

All customer data at rest is stored encrypted.

Any file system storage of customer data, either encrypted or unencrypted, is avoided. Multi-Bank Connectivity uses Sybase ASE for the main data storage, whereas the Business Cockpit uses HANA DB. Data stored in Sybase is encrypted using AES and a key length of 128 Bits. The encryption key is automatically generated, unique for each tenant, and is not stored in the same database as the encrypted data. Data stored in Hana DB is encrypted using AES and a key length of 256 Bits. Data stored on the Multi-Bank Connectivity-hosted FTP server (vendor Cleo) is encrypted as a result of the Multi-Bank Connectivity messages already being encrypted.

Data stored temporarily at rest (that is, stored in the file system during payment instruction processing) is also encrypted. Temporary file system storage can be used when a certain message size is exceeded. It is done to circumvent restrictions on physical and virtual memory during payment instruction processing. Temporary file system storage is only for a short time, that is, a few seconds.

Multi-Bank Connectivity stores Multi-Bank Connectivity messages for 90 days.

1.3.2.3 Data Transmission and Data Flow Control

All data in transit, either exchanged with customers or internal, is encrypted.

At the transport layer, TLS and SSH are leveraged. For security reasons, SSL is disabled and TLS is used instead. TLS protects HTTP-based communication using a symmetric key length of at least 128 bits, which is technically enforced. SSH also uses a key length with at least 128 bits to protect FTP communication. The asymmetric key length used in TLS and SSH is typically 2048 bits, but at least 1024 bits.

At the message layer, data encryption is mandatory. A deviation from this rule by individual customer agreement requires a discussion with the Multi-Bank Connectivity security team. Message-layer encryption is achieved using various algorithms and key lengths. The available algorithms include AES, DES, RC2, and Camellia. Strong encryption can be used for AES and Camellia using a key length of 192 and 256 bits.

Digital signatures are leveraged to detect both unintentional and intentional Multi-Bank Connectivity message changes.

Use of X.509 Certificates and PGP Keys

HTTPS communication at the message entry of Multi-Bank Connectivity is secured using X.509 client certificates. Some of the Certificate Authorities (CAs) that are currently supported are *TC TrustCenter CA* and

Verisign Class3 Public Primary certificate Authority - G5. For a complete list of currently supported CAs, see the link in chapter Further Information [page 53]. Additional CAs can be added on customer demand and after evaluation by the Multi-Bank Connectivity security team. Certificates are also used in various other use cases, such as digital signatures.

Multi-Bank Connectivity uses *Verizon Public SureServer CA G14-SHA2* for issuing certificates that represent parts of Multi-Bank Connectivity, for example, a tenant.

Requirements for Cryptographic Keys

For both transport-level and message-level security, Multi-Bank Connectivity requires two different key pairs.

Multi-Bank Connectivity strongly recommends using public keys that are signed with SHA-2, rather than SHA-1. Multi-Bank Connectivity recommends that asymmetric keys are at least 2048 bits long.

Multi-Bank Connectivity recommends using an expiration time of three years for public keys.

For transport-layer security, CA-issued certificates are mandatory. For message-layer security, CA-issued certificates are recommended, although self-signed certificates can be used.

Handling of Cryptographic Keys

Public key material (certificates) is exchanged between SAP and customers during onboarding to Multi-Bank Connectivity.

For security reasons, keys associated with tenants are not stored in the file system. Instead they are stored in a database, leveraging the platform's keystore service. Keys are protected using a strong password.

When Multi-Bank Connectivity Cloud Operations generates a key pair consisting of a public key and the corresponding private key, and subsequently issues a certificate signing request, this all happens within a dedicated secure environment only used for this purpose. These activities are performed on a dedicated system (a static virtual machine) that is only reachable using Windows Terminal Server (WTS). Only certain operators in Multi-Bank Connectivity Cloud Operations have permission to perform these tasks. Before key material is brought into the platform's runtime, that is, into keystore service, it is stored in a secure third party solution (Password Depot) specifically designed for storing key material. This solution is set up to allow fine-grained permission, logging, alerting, and notification for any activity.

The keys of the load balancer and the Multi-Bank Connectivity-hosted FTP server are stored securely in the file system of these components.

1.3.2.4 Isolation and Multitenancy

Each SAP Multi-Bank Connectivity customer is assigned its own tenant. The SAP Multi-Bank Connectivity message processing runtimes of different customers are located on different virtual machines. Data of different customers stored in the database is put into different database schemas.

The internal network only allows specific communication (HTTPS) from one virtual machine to another, and this only by taking the loop to the load balancer. Furthermore, internal components of SAP Multi-Bank Connectivity are placed in different network segments: sandbox and services.

SAP Multi-Bank Connectivity maintains two landscapes that serve different purposes. These landscapes are isolated from each other.

Landscape	Purpose
TEST	Standard test cluster for customers who have purchased an HCI or SAP Multi-Bank Connectivity license
PROD	Standard Prod cluster for customers who have purchased an HCI or SAP Multi-Bank Connectivity license

Related Information

Tenant Isolation [page 14]

1.3.2.5 Cryptographic Algorithms Used by Multi-Bank Connectivity

In its standard configuration, Multi-Bank Connectivity uses the following encryption/signing algorithms.

Data Lifecycle	Layer	Encryption/Signing Means	
Data in transit	Transport Layer	TLS	SSH

Data Lifecycle	Layer	Encryption/Signing Means		
		• AES128-SHA256 • AES256-SHA256 • AES128-SHA • AES256-SHA	• BLOWFISH-CBC • 3DES-CBC • AES128-CBC • AES128-CTR • AES192-CBC • AES192-CTR • AES256-CBC • AES256-CTR • ARCFOUR128 • ARCFOUR256 • CAST128-CBC • TWOFISH128-CBC • TWOFISH192-CBC • TWOFISH256-CBC	
	Message Layer	PKCS#7	PGP	XML Digital Signature
		• AES/CBC/PKCs5Padding • SHA512/RSA	• AES/ ZLIB	• SHA512/RSA
Data at rest	n/a	Sybase • AES128 HANA DB • AES-256-CBC SFTP Server • Same as data in transit/ message layer Temporary files in file system RC4		
Data in processing (in memory)	n/a	No encryption/signing		

FIPS 140-2

Multi-Bank Connectivity aims to use only cryptographic algorithms listed in *Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology.

The security module used in the Multi-Bank Connectivity cloud environment is not FIPS 140-2 certified. On the corporate side, the connector for the SAP Multi-Bank Connectivity can be configured to use a certified cryptographic module. To do so, you must apply 2117112.

1.3.2.6 Security by Component

Connector for the SAP Multi-Bank Connectivity

The connector for the SAP Multi-Bank Connectivity provides easy connectivity and integration to corporate customers when connecting to Multi-Bank Connectivity. It can be installed in an SAP ERP system and facilitates the appropriate security settings, for example, message-level security and the length of the encryption key. The connector is built on the security capabilities of the SAP ERP 6.0 system. The connector provides encryption/decryption and signing/verification. The security key material used by the connector is stored in PSEs (Personal Security Environment). The security-related settings are administrated using transactions STRUST and SSFA.

1.3.3 User Interface Security

Multi-Bank Connectivity Cloud Operations uses an Eclipse-based operations UI, in combination with UIs of the Hana Cloud Platform (HCP).

These user interfaces are built in such a way that they prevent vulnerabilities such as cross-site-scripting (XSS) and cross-site-request-forgery (XSRF). The built-in security capabilities of these technologies are used together with secure design and coding principles.

1.3.4 Layers of Information Security

1.3.4.1 Layer 1: Physical Site

SAP data centers are world-class data centers. The data center in St. Leon-Rot, Germany, from where Multi-Bank Connectivity is offered, has redundant power supplies (diesel engines), aspirating smoke detectors (ASD), fingerprint access control, and 24-hour surveillance.

Ceilings, walls, and doors provide 90 minutes of fire resistance. A fire-extinguishing system based on gas (INERGEN) is in place. All of these measures are regularly checked and audited. The data center hosts solutions that provide various certifications such as ISO27001 (certification for the operation of software), ISO22301 (Business Continuity management), and SSAE 16 (U.S. equivalent of ISAE 3402).

1.3.4.2 Layer 2: Database

Multi-Bank Connectivity stores its data in SAP Sybase ASE (Adaptive Server Enterprise), running in a high-availability setup as well as in HANA DB. Data of different customers is put into different database schemas. All customer data, as well as cryptographic key material, is stored encrypted.

Data from the primary data center Germany/Rot is backed up to Germany/ Walldorf 14 km away, where SAP's headquarters are located. The corresponding backup data/log files are generally moved to a backup device in the geographically separate backup data center.

A full backup is performed daily. Incremental backup of the database files is triggered at least every 30 minutes. This data (corresponding backup data/log files) is moved to a backup device every two hours. SAP's data backup and restore processes comprise regular backups on redundant media.

Related Information

Data Storage and Location [page 42]

1.3.4.3 Layer 3: Middleware

SAP Multi-Bank Connectivity uses SAP HANA Cloud and SAP Integration Suite as platform and middleware, respectively.

SAP HANA Cloud supports multi-tenancy, virtualization, and lifecycle capabilities for the applications and scenarios. Furthermore, the platform offers services such as a persistency service and a keystore service. SAP Integration Suite provides enhanced security capabilities, for example, it supports various encryption standards such as PKCS#7 and PGP. In addition, SAP Integration Suite can run integration content that realizes various communication patterns, also known as enterprise integration patterns. Examples of enterprise integration patterns are asynchronous communication, synchronous communication, routing patterns, and transformation patterns.

1.3.4.4 Layer 4: Application

The Multi-Bank Connectivity application consists of software that runs on different nodes. A node is assigned to a virtual machine.

The runtime node performs Multi-Bank Connectivity message processing. The tenant management node is used by the tenant administrator, whereas the central management node is used by the SaaS administrator for central administration tasks. The software consists of Java code provided by SAP as well as publicly available open source code. Multi-Bank Connectivity implements a fine-grained permission concept that facilitates the least-privilege principle and segregation of duties by separating powerful permissions into different personas.

1.3.4.5 Layer 5: Network and Communication

The external facing network is divided into multiple demilitarized zones (DMZ). A multilevel firewall filters and blocks suspicious incoming traffic. An intrusion prevention system (vendor HP TippingPoint) detects potential intrusion attempts. A load balancer (vendor F5) terminates TLS and distributes the requests.

Multi-Bank Connectivity consists of certain components that are only internally used, for example, by the SaaS administrator. The access points of these components are separated from the externally accessible components. These internally used components are thus not externally visible and not externally accessible.

1.3.5 System Operations

Multi-Bank Connectivity is operated by Multi-Bank Connectivity Cloud Operations and supported by a dedicated Multi-Bank Connectivity Support team. Both are units within SAP. Multi-Bank Connectivity Cloud Operations is located in Bangalore, India. Multi-Bank Connectivity Cloud Operations are on duty 24*7*365.

An alerting infrastructure is used to detect any anomaly in the system and operators act on these alerts. Access rights of operators are constantly monitored, reviewed, and minimized. There are defined and communicated maintenance *windows* in which system updates and changes are applied.

1.3.5.1 Permissions of Operators

Multi-Bank Connectivity Cloud Operations is separated into two subgroups: The smaller productization team and the larger operations team.

The productization team takes care of conceptual activities such as introducing new procedures, while the operations team performs system operations. The productization team has more powerful permissions than the operations team. Neither team is involved in activities that require them to look at Multi-Bank Connectivity messages.

1.3.5.2 Interaction with Customers

Interaction with customers is exclusively handled by the Multi-Bank Connectivity Cloud Services Center team, who also perform onboarding activities for new customers.

Multi-Bank Connectivity Cloud Operations does not interact with customers.

1.3.5.3 System Changes

All changes to the system must be approved, and are made in a controlled manor, that is, they are planned, tested, scheduled, and applied.

Several processes are involved, for example, the change management process, integration content lifecycle process, correction process, and release deployment process. The process steps of these processes are tracked and traced.

1.3.5.4 Handling of Cartridges

To perform runtime transformations from one message format to another, Multi-Bank Connectivity uses cartridges provides by a third party vendor.

In order to introduce a new transformation (aka message mapping), the Multi-Bank Connectivity teams provide a specification to the third party vendor. The third party vendor then provides a cartridge containing the message mapping on an SFTP server that they operate. The cartridge is then picked up by the Multi-Bank Connectivity Cloud Service Center team and applied to the respective tenants.

1.3.5.5 Audit Logging

Audit logs are generated for each tenant. This means that data of different customers is not mixed.

The audit log contains entries for configuration changes and security events, such as failed authentications. The audit log is stored in a third party audit log system (vendor Splunk) operated by SAP. The system implements strict access control and log modification prevention. Audit logs are retained for 18 months. Audit logs can be provided to the customer on request. The load balancer as well as the intrusion prevention system also log in to Splunk.

1.3.5.6 Periodic Checks

In order to ensure a permanent high level of security, Multi-Bank Connectivity Cloud Operations performs a set of periodic monthly checks.

Among other things, these verify the permissions currently granted, revoke any unneeded permissions, change passwords, and check cryptographic key material for upcoming expiration.

1.3.6 Data Protection and Data Privacy

The primary data center in St. Leon-Rot is subject to the data protection and privacy law of Germany.

Customer data processed by Multi-Bank Connectivity is classified as confidential. Processing personal data is not part of the core functionality of Multi-Bank Connectivity. Multi-Bank Connectivity can however receive

personal data as part of payment instructions. An example is a payment instruction sent by a corporation to a bank, where the payment beneficiary is a natural person. A part of the personal data, for example, account numbers, are classified as sensitive personal data.

1.3.6.1 Multi-Bank Connectivity as Data Processor

When a corporation or bank signs up to Multi-Bank Connectivity and later exchanges payment instructions with Multi-Bank Connectivity, they always assume the role of the data controller for personal data.

As such, the corporation or the bank has a responsibility towards the data subject for handling personal data. It is also obliged to be able to respond to inquiries from the data subject regarding the type and amount of stored data, and to requests for data deletion. Multi-Bank Connectivity processes personal data and data in general on behalf of a corporation or bank and acts as data processor.

1.3.6.2 Multi-Bank Connectivity as Data Controller

As well as data contained in Multi-Bank Connectivity messages, there are other types of data where Multi-Bank Connectivity assumes the role of a data controller.

1. Customer data collected during onboarding to Multi-Bank Connectivity (during the process of setting up the connection between the customer system and Multi-Bank Connectivity)
   Examples: Name, role, e-mail address, and contact phone numbers of customer contacts directly involved in the day-to-day interactions and tasks that are needed to support onboarding to Multi-Bank Connectivity.

1.3.6.3 Third-Party Subprocessors for Personal Data

Multi-Bank Connectivity maintains subprocessor agreements with a set of third-party companies (non-SAP Affiliates).

Currently, there are a few third-party subprocessors, who mainly provide technical services and support. In order for Multi-Bank Connectivity to employ a subprocessor, SAP passes its obligation as data controller or processor to the subprocessor. During the selection and engagement process for a new subprocessor, existing Multi-Bank Connectivity customers will be informed and can object to the appointment of an additional subprocessor.

1.3.6.4 Upcoming European General Data Protection Regulation

In compliance with the upcoming European general data protection regulation, a dedicated European Multi-Bank Connectivity Cloud Operations team will operate the systems of European customers that contain encrypted data.

Personal data in Multi-Bank Connectivity will only be accessible to these operators and not to operators outside of Europe. This is currently being set up.

1.3.7 Security Controls and Practices

There are various controls and practices that are employed to ensure information and software security.

1.3.7.1 Conclusion

The comprehensive security measures described here equip Multi-Bank Connectivity to provide a trusted, secure, and reliable service. The security of Multi-Bank Connectivity is constantly evolving in line with new security trends and practices, new customer requirements, and industry trends.

1.3.7.2 Information Security Incident Management

Security incidents are handled according to the Security Incident Management Process.

This process foresees classification, containment and resolving of the issue. Internal groups and decision takers are pulled in as needed. Trending is performed on security incidents as part of the quarterly ISO27001 performance report. Customers can on request be provided with a report on security incidents.

1.3.7.3 Consistently proven Security Measures

Vulnerability Assessments and Penetration Tests

Vulnerability assessments and penetration tests are executed regularly by 3rd parties in request of SAP. Penetration tests focus on the network and infrastructure layer, whereas vulnerability assessments focus on Multi-Bank Connectivity business functionality.

Virus Scanning

Virus scanning is enabled at the Multi-Bank Connectivity-owned and -operated SFTP Servers.

1.3.7.4 Security Education and Awareness

Everyone involved in Multi-Bank Connectivity is regularly educated by awareness trainings on the importance and relevant of security. Software developers are especially skilled by secure programming trainings.

1.3.7.5 Compliance Standards

SAP Multi-Bank Connectivity is compliant with various SAP-internal technical policies, procedures, directives, guidelines, and product standards. For more information, please visit the SAP Trust Centre and search for SAP Multi-Bank Connectivity.

1.3.7.6 Secure Software Development

The development of Multi-Bank Connectivity follows the SAP Security Development Lifecycle (SDLC).

As part of this, regular quality gates need to be passed. Source code is monthly scanned for security issues using HP Fortify, audited and fixed. Threat modeling is selectively applied and a general focus on security architecture and design is placed. In addition the SAP-internal product standard requirements for security are applied.

When Open Source Components are used, they are scanned for security vulnerabilities based on a risk assessment. In addition the NIST National Vulnerability Database is used to check for known vulnerabilities and apply fixes as appropriate.

1.3.7.7 Reports that can be provided to Customers

The following reports provide customers with visibility into Multi-Bank Connectivity and into their tenant. The reports can be provided to customers on request:

- Message Processing Report
- Service Availability Report
- Configuration Change Report
- Security Incident Report

1.3.8 Disclaimer

This document provides forward-looking statements marked as *planned*. This means that the Multi-Bank Connectivity team intends to provide the mentioned capability. However, this should not be understood as a commitment nor as a specific timeline.

1.3.9 Further Information

SAP Multi-Bank Connectivity Solution Overview

SAP Multi-Bank Connectivity product page

Certificate Authorities Supported by SAP Multi-Bank Connectivity

List of Trusted Certificate Authorities

SAP Security Development Lifecycle

http://www.sap.com/search/search-results.html?Query=SAP+Security+Development+Lifecycle

Select The Security Development Lifecycle at SAP from the search result list.

Connector for the SAP Multi-Bank Connectivity

https://help.sap.com/mbc

1.3.10 Contacts

Multi-Bank Connectivity Solution Management

Multi-Bank Connectivity Marketing

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP