



PUBLIC
2024-03-22

Product Assistance for SAP Multi-Bank Connectivity

Content

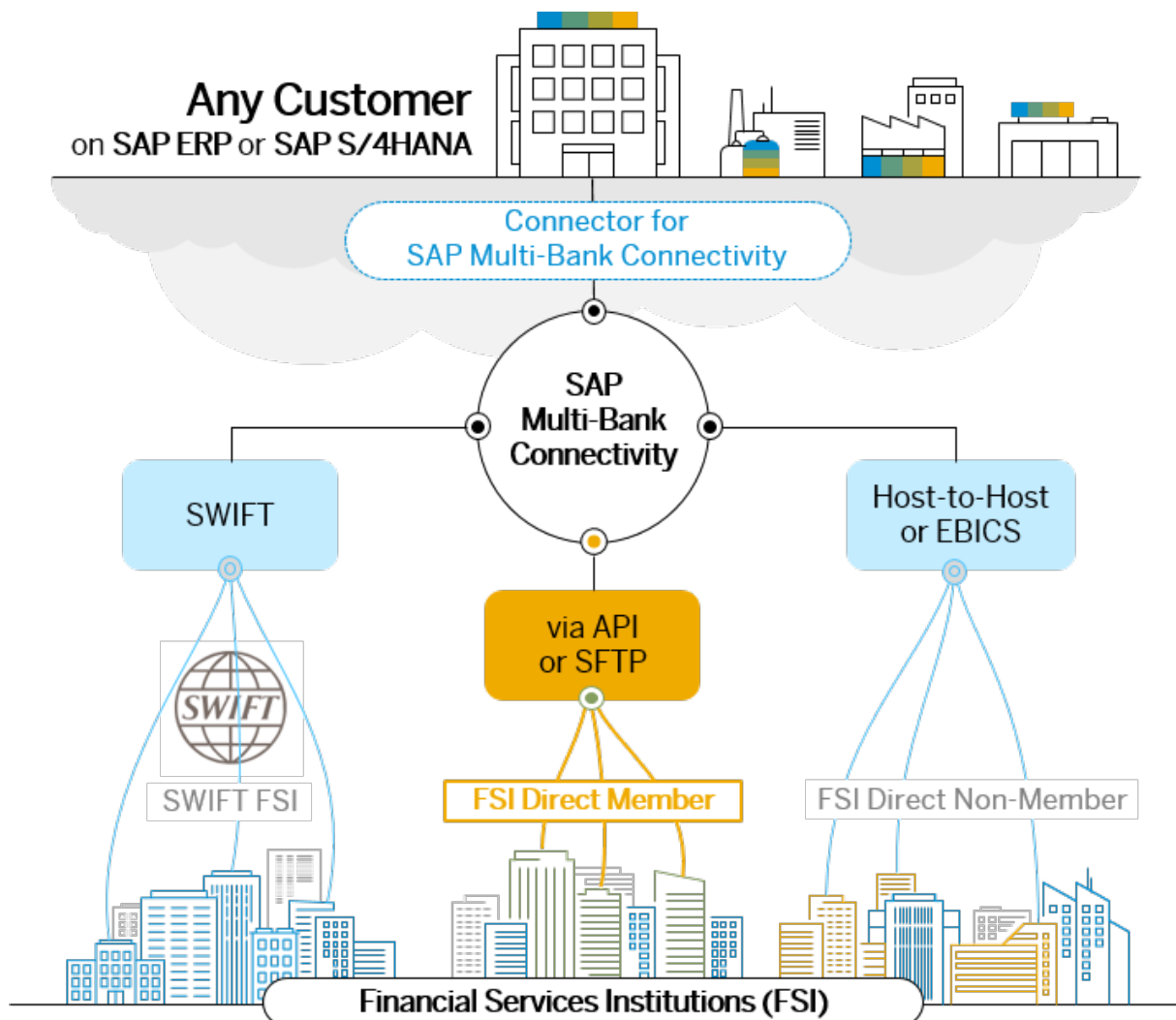
- 1 SAP Multi-Bank Connectivity 3**
- 1.1 Product Overview. 5
 - SAP Multi-Bank Connectivity System Landscape 6
 - Capabilities. 6
 - Service Consumption. 18
- 1.2 Security Capabilities. 19
 - Certificate Requirements and Trusted Certificate Authorities. 21
 - SAP Multi-Bank Connectivity Security Datasheet. 25
- 1.3 Onboarding Process. 40
 - Roles and Responsibilities. 42
 - Connection Setup During Onboarding. 43
- 1.4 Support Information. 50
 - Notifications via S-User ID. 52
 - Roles and Responsibilities in Support or Incident Case. 54
 - Escalation Path. 55

1 SAP Multi-Bank Connectivity

SAP Multi-Bank Connectivity is an SAP Business Technology Platform (BTP) solution managed by SAP to provide customers connectivity with their banks.

Use

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.



For the integration between the customer's SAP system and SAP Multi-Bank Connectivity, the connector for SAP Multi-Bank Connectivity is utilized. All messages to and from SAP Multi-Bank Connectivity pass through the connector. Message monitoring is available at the connector for SAP Multi-Bank Connectivity using either

the classical Connector Monitor (/BSNAGT/MONITOR, for releases before SAP S/4HANA 1909 FP01) or the Manage Bank Messages SAP Fiori app (starting at SAP S/4HANA 1909 FP01 or SAP S/4HANA Cloud). Each message sent through the connector for SAP Multi-Bank Connectivity has a Sender ID, Receiver ID, message type, filename, message content, as well as other context information, such as SWIFT parameters or approval user information required for the integration towards the banks.

Features

SAP Multi-Bank Connectivity supports the exchange of all types of messages. The most relevant sources of messages are automated, but other sources and message types can also be sent to the cloud service or can be received.

Outbound Messages from SAP System to Bank

The available integration scenarios for outbound communication are as follows:

- Payments from:
 - Payment Run
 - FI-CA
 - Employee Central Payroll
 - Advanced Payment Management
- Treasury confirmations
- Generic file pickup

When the settings of the payment format indicate to send the message to SAP Multi-Bank Connectivity, no physical payment file is created – instead, a message is created within the connector for SAP Multi-Bank Connectivity. This message includes the payment format content. After connectivity between the connector and SAP Multi-Bank Connectivity has been established, the message is immediately sent from the connector to SAP Multi-Bank Connectivity and then on to the bank.

For more information, see [Outbound Payment Processing](#).

Inbound Messages from Bank to SAP Customer

Because SAP Multi-Bank Connectivity is closely integrated with the SAP back-end system, it can seamlessly update various other modules in the SAP system once the messages are available from the banks.

The process is as follows:

- The Pull Messages report running as a scheduled job (/BSNAGT/MESSAGES_PULL) is executed to pull messages from SAP Multi-Bank Connectivity.
- The message is processed by the respective business process triggered by the connector for SAP Multi-Bank Connectivity based on the message type.

Based on the message type, the system either triggers automatic processing or triggers a download to a file directory or sets the status of the message to indicate that manual processing is required.

Supported processes for automated processing include the following:

- Payments
 - Payment messages (all formats)

- Status messages
- Intraday Statements
- End of day Statement
- Lockbox
- Confirmations
 - MT300 /MT320
- Bank fee reports
 - Bank Service billing

All other processes are for manual processing in the connector for SAP Multi-Bank Connectivity.

For upcoming features, see the [SAP Road Map Explorer](#) for SAP Multi-Bank Connectivity.

1.1 Product Overview

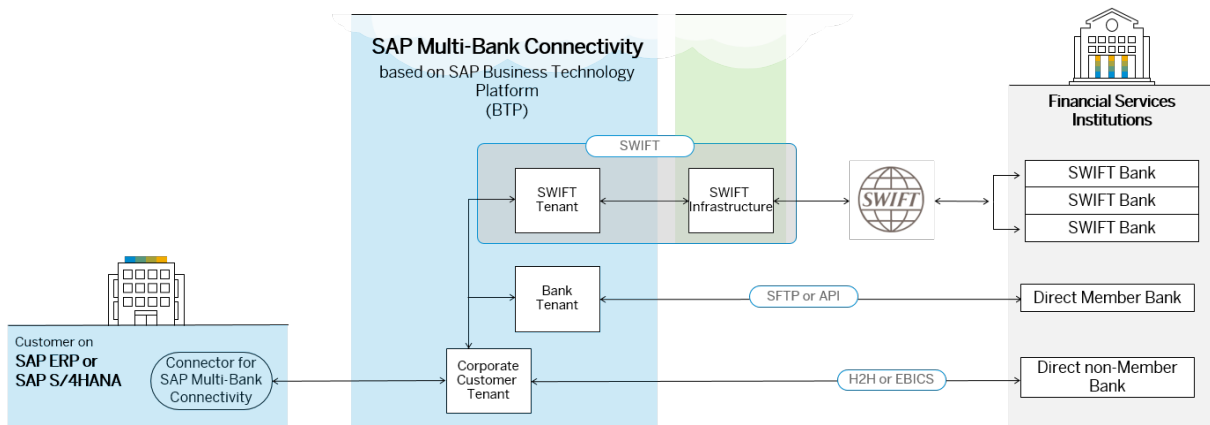
SAP Multi-Bank Connectivity directly connects corporates with financial services institutions.

The solution provides corporates with a multibank, digital channel between their ERP systems and their banks. Besides that, the solution also offers embedded SWIFT connectivity.

This corporate cloud banking network provides measurable improvement to the accounts payable and accounts receivable functions through automation of all the manual and error-prone steps associated with the execution and reconciliation of payments, order-to-cash applications, and order entry documents.

The use of SAP Multi-Bank Connectivity results in improved control, efficiency, and transparency of the financial accounting process. As the solution automatically updates payment status and cash positions in the ERP system once updates are available from the banks, it further improves and streamlines the company's treasury operations.

The onboarding to the solution is very straight-forward and delivered through a private cloud owned and managed by SAP that is secure and partitioned by each customer and their network of banks.

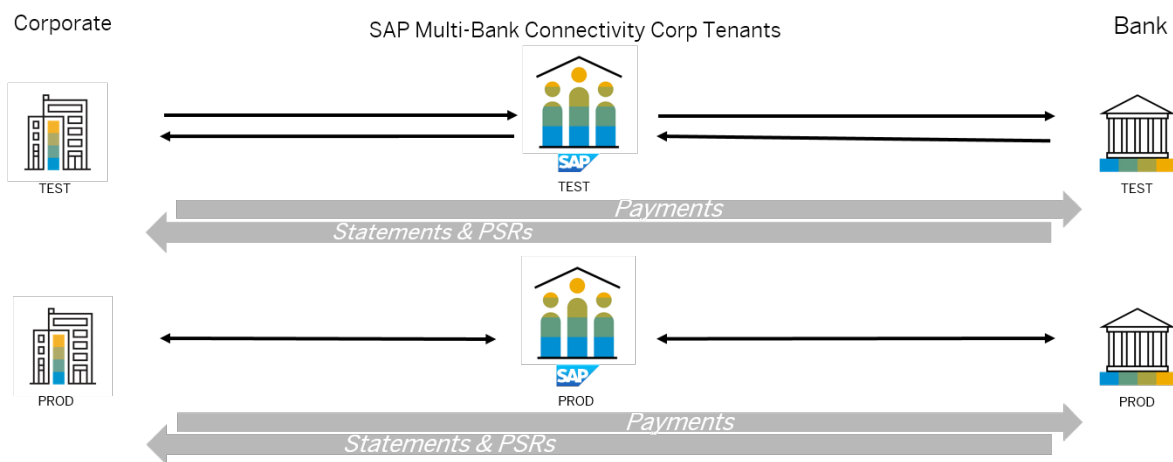


1.1.1 SAP Multi-Bank Connectivity System Landscape

SAP Multi-Bank Connectivity exposes two system landscapes: test and production.

These should be integrated with the corresponding systems, that is, test to test and production to production on the customer side. SAP Multi-Bank Connectivity test and productive systems are isolated from one another and are further secured by using different security artifacts.

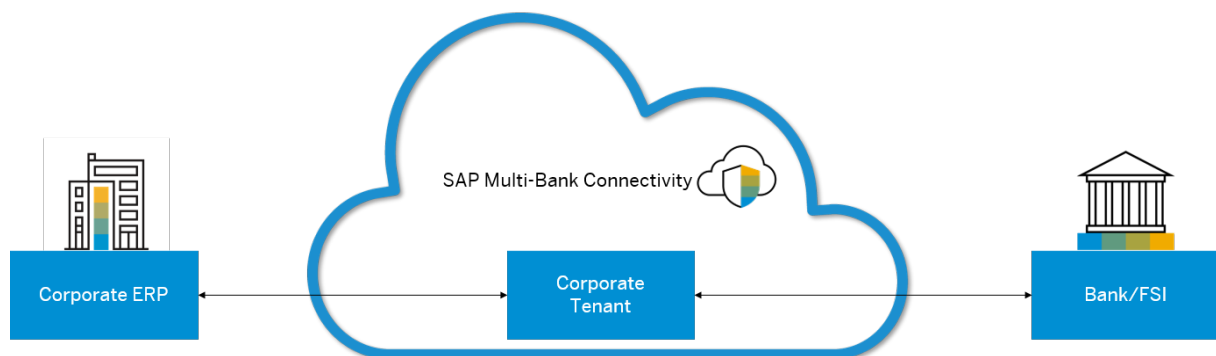
Demonstration of the SAP Multi-Bank Connectivity Landscape – Test Versus Production



1.1.2 Capabilities

SAP Multi-Bank Connectivity provides a number of different capabilities or options to connect your ERP system to your financial services institutions (FSIs).

There are two connections that need to be setup when you get onboarded to SAP Multi-Bank Connectivity: the first from your ERP system to SAP Multi-Bank Connectivity, and the second from SAP Multi-Bank Connectivity to your banks or FSIs.



Related Information

[Onboarding Process \[page 40\]](#)

1.1.2.1 SWIFT

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a member-owned cooperative that provides safe and secure financial transactions for its members.

SWIFT has established connections to thousands of banks. Many SAP customers want to connect to the SWIFT network from SAP. This is possible using SAP Multi-Bank Connectivity, without any additional software or hardware footprint on the customer's side. A third-party service provider (for example, typically a SWIFT service bureau) is no longer needed for SAP customers to send and receive messages over the SWIFT network.

SAP is a SWIFT Alliance Lite2 for Business Applications (L2BA) provider. In this model, SAP operates the SWIFT infrastructure and standardized integration for customers with a valid SWIFT agreement, using SAP as an L2BA provider in place.

1.1.2.1.1 Corporations Using SWIFT via SAP Multi-Bank Connectivity

SAP Multi-Bank Connectivity seamlessly integrates into the SWIFT network, which allows SAP customers to leverage the bank reach that the SWIFT network provides.

Use

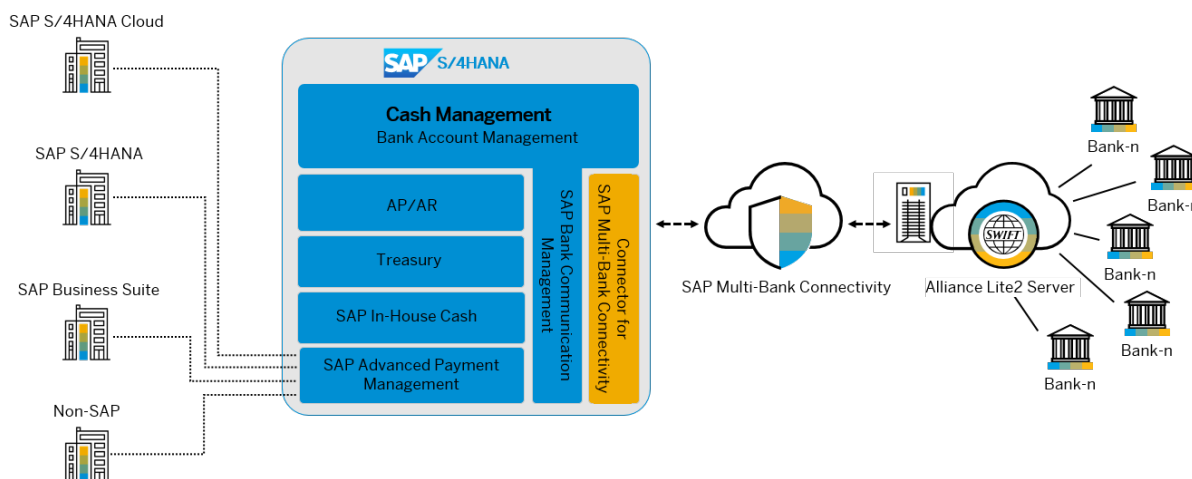
Note

An SAP customer wanting to connect to the SWIFT network from SAP must have membership to SWIFT, such as SWIFT Alliance 2. SAP is not a reseller of SWIFT so corporates must subscribe separately to SWIFT to get their BIC code or ask for migration of their existing BIC and sign an agreement to cover messages passed via SWIFT.

To establish the connection with SWIFT, SAP operates SWIFT software, SWIFT-specific hardware, and dedicated Internet connections to SWIFT. SAP Multi-Bank Connectivity and the connector for SAP Multi-Bank Connectivity use this setup for the connection between the corporate customer (SAP ERP system) and the banks.

In addition, SWIFT parameters are added via configuration in the connector for SAP Multi-Bank Connectivity. These parameters are passed as additional attributes with the message to SAP Multi-Bank Connectivity. Setting the parameters for messages going over the SWIFT network will be covered in the respective section of the Configuration Guide of connector for SAP Multi-Bank Connectivity. SAP supports both FIN and FileAct-based communication.

On the inbound side, from the SWIFT network to a corporate customer, SAP Multi-Bank Connectivity receives the messages from the SWIFT network. After validating the message signature, SAP Multi-Bank Connectivity forwards these messages without a SWIFT-specific XML envelope to the connector for SAP Multi-Bank Connectivity in the respective SAP ERP system. Acknowledgments and delivery notifications are mapped to an ISO 20022 PAIN.002 format before they get forwarded to the ERP system to allow automated processing. The acknowledgments are pushed to the SAP Bank Communication Management module where reporting on payment batches and corresponding status messages is available.



Related Information

[Configuring SWIFT Parameters for connector for SAP Multi-Bank Connectivity](#)

1.1.2.1.2 SWIFT Message Types: FIN and FileAct

SAP Multi-Bank Connectivity supports both FIN and FileAct-based communication.

- FIN enables the exchange of messages formatted with the traditional SWIFT MT standards. FIN works in store-and-forward mode, which makes it easy to exchange messages with a large number of correspondents, many of whom may not be online at the time of transmission. Store-and-forward removes the uncertainty and inconvenience of worrying about whether or not your correspondents are online at the time you send the message. Your message is delivered as soon as the recipient is ready to receive it.
- FileAct transfers any type of data, such as text, spreadsheet, XML formatted files, and images. It supports all types of character sets and any content structure – you can use SWIFT message formats MTs or MXs, domestic formats, or your own proprietary ones. Files of almost any format or size may be sent, up to hundreds of MB.

Please note that for outbound messages to SWIFT, only US-ASCII characters are supported in the file names.

Note

For more information about pricing, corporates must contact their SWIFT account manager. Additional documentation about the evolution and the usage of FIN and FileAct is available on swift.com:

- [Solutions](#) > [Release timeline](#) >
- [Support](#) > [Documentation](#) >

1.1.2.1.3 SWIFT Customer Security Programme (CSP) in the Context of SAP Multi-Bank Connectivity

To proceed with an SAP Multi-Bank Connectivity integration via SWIFT, the SWIFT Customer Security Program (CSP) must be in place. This is a prerequisite to any entity that transmits data to or from the SWIFT network.

What Is the SWIFT CSP?

The SWIFT CSP is designed to be a collaborative effort between SWIFT and its users to strengthen the overall security of the financial ecosystem against cyber attacks. All users must therefore take the following three main steps:

1. Understand SWIFT's Customer Security Controls Framework (CSCF), including the mandatory and advisory security controls. You can access reference documents and training on [swift.com](https://www.swift.com) and join customer security webinars.
2. Start a project to assess your compliance with the security controls and close any gaps. This will strengthen your local footprint security and your connection to SWIFT, helping to protect you and your counterparts against cyber threats.
3. Attest your level of compliance with the controls annually between July and December 31st. You can do this via the KYC Security attestation application (KYC-SA) on [swift.com](https://www.swift.com). You don't need to have implemented all the controls to submit your attestation. You can do it straight away, identifying target dates when possible, and update it once your security project is complete.

How can I Initiate the CSP Attestation?

You can find all relevant information on the SWIFT CSP [website](#) .

How Long is the Timeline for the CSP Attestation to be Completed?

The maximum timeline for this process to be completed depends on whether your company is a new or a migrating SWIFT customer.

- **New SWIFT customers:** If you're a corporate customer that just signed up for your first SWIFT BIC, please be aware that a valid SWIFT CSP attestation for architecture type A4 must be completed in order to move on to the promotion phase of the SAP Multi-Bank Connectivity onboarding project. If you're not in compliance with this requirement, your company won't be allowed to go-live via SWIFT.

- **Migrating SWIFT customers:** If your company is already a SWIFT customer and you'd like to connect your existing SWIFT BIC to SAP Multi-Bank Connectivity, it's very likely you already have a valid SWIFT CSP attestation in place for the pre-existent setup. If this is the case, your valid CSP for the pre-existent setup will be sufficient for going live with SAP Multi-Bank Connectivity. However, from the go-live date to your new service provider (SAP Multi-Bank Connectivity), your company will have three months to adjust the SWIFT CSP attestation to the new architecture type A4.

To check the status of the SWIFT CSP attestation, please contact your SWIFT account manager or regional contacts.

What Type of Controls Are in Scope in the CSP when Integrating SWIFT via SAP Multi-Bank Connectivity?

With regards to the controls in scope in the SWIFT CSP attestation, these are determined by the SWIFT architecture type, defined by how SWIFT members (corporates) connect to the SWIFT network. In the context of SWIFT integration via SAP Multi-Bank Connectivity, corporate customers need to select the following:

- *Architecture Type:* Architecture type A4
- *Service provider type:* Alliance Lite2 for Business Applications
- *Business application provider name:* SAP

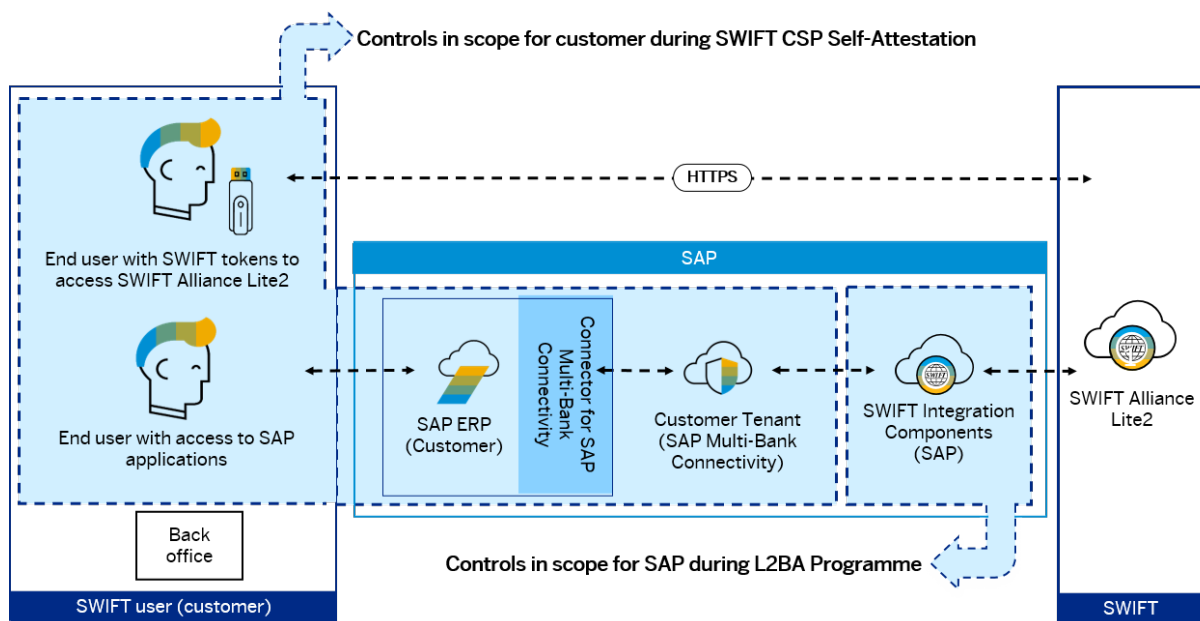
By selecting these criteria, the controls in scope for the CSP attestation will focus on

- the corporate customer's infrastructure, such as the operator's PC or workstations, and the devices used by the corporate customer's users to access SWIFT via SAP ERP or the SWIFT GUI/RMA directly with SWIFT tokens.
- the corporate customer's SAP Multi-Bank Connectivity tenant.

Note

You can use existing certifications to answer any questions for your self-attestation. For more information, please see [SAP Compliance Offerings](#).

These controls are not focusing on SAP's infrastructure integrating with SWIFT as this is already covered by SAP under the partnership agreement with SWIFT.



Note

To verify if SAP SE has a valid certification with SWIFT as part of their L2BA partnership, check the [SWIFT Compatible Applications Finder](#).

Who Can Be Considered as Independent Assessor for This Process?

Since July 1st, 2021, the SWIFT CSP has become an 'independent assessment framework', which means that it can only be conducted by a certified external auditing firm or certified internal resources. **Please note that SAP is not acting as an independent assessor for this process.**

- If you opt for an external assessment, consider consulting the SWIFT Directory of CSP assessment providers on [swift.com](#).
- If you opt for an internal resource, you must make sure that they have the right skills and certifications and are in a department that is independent from the one using or implementing the system (such as the Compliance Office, Risk Office, or Internal Audit).

What Type of Certifications Is an Independent Assessor Required to Have?

Independent assessors, whether external or internal, must have recent, relevant experience within cyber security, working with an industry standard such as PCI DSS, ISO/IEC 27001, or the NIST Cybersecurity Framework, and must have an industry-related professional certification, for example, CISSP, CISA, CISM, ISO/IEC 27001 Lead Auditor, or QSA. For the full list of criteria, see the SWIFT CSP website or ask your SWIFT contact.

Who Can Support Me with My SWIFT CSP?

If you require further assistance with your SWIFT CSP attestation submission, you can contact SWIFT Support via Case Manager:

1. Log in to [MySWIFT](#).
2. On the top-right side of the page, choose [My tools](#).
3. Under [Support](#), choose [Case Manager](#).
4. Choose the [Report a case](#) tab.
5. Complete the form.

You can also call the SWIFT Support [helpline](#) .

Note

SWIFT Support won't be able to advise on the specific answers that each corporate customer will be required to provide, but they can help with the interpretation of the controls in scope for the CSP attestation questionnaire.

Related Information

[MySwift](#) 

[SAP Compliance Offerings](#) 

1.1.2.2 Direct Bank Integration

There are two ways a direct bank integration can be set up. Either customer ERP systems are directly connected to the banks in scope via SAP Multi-Bank Connectivity, or the banks to be connected are an SAP Multi-Bank Connectivity member bank with their own MBC tenant. For more detailed information, please see the next topics.

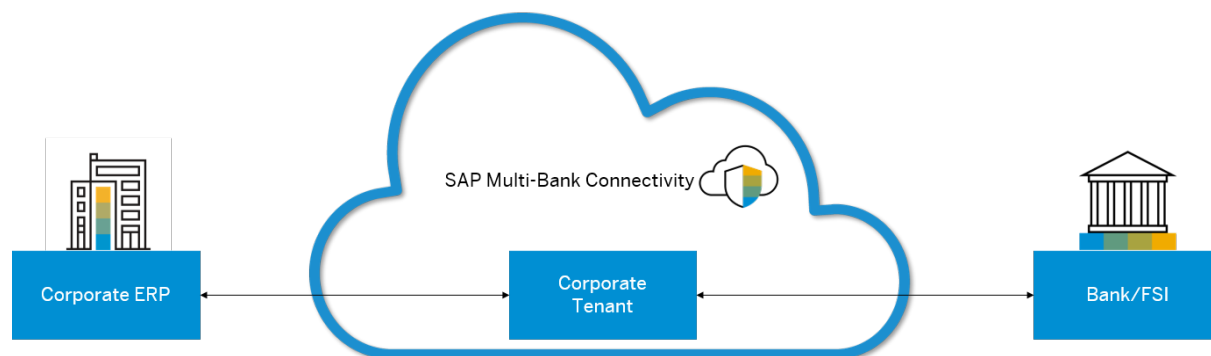
Related Information

[Host-to-Host \[page 13\]](#)

[Member Banks \[page 13\]](#)

1.1.2.2.1 Host-to-Host

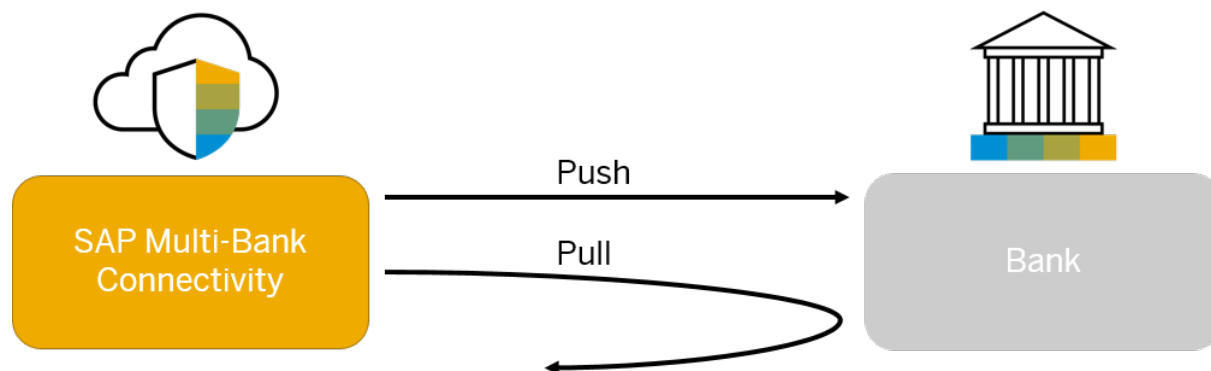
A host-to-host connection sends messages from the corporate system to the corporate tenant and then to a bank back-end system.



For integrating your tenant directly to your bank, SAP Multi-Bank Connectivity generally offers connectivity via **Secure File Transfer Protocol (SFTP)**.

SAP recommends a bank-hosted SFTP connectivity for message exchange as it provides simple and effective scalability options.

In this scenario, SAP Multi-Bank Connectivity pushes data to a bank's hosted server, and SAP Multi-Bank Connectivity pulls response data from the bank's server.



1.1.2.2.2 Member Banks

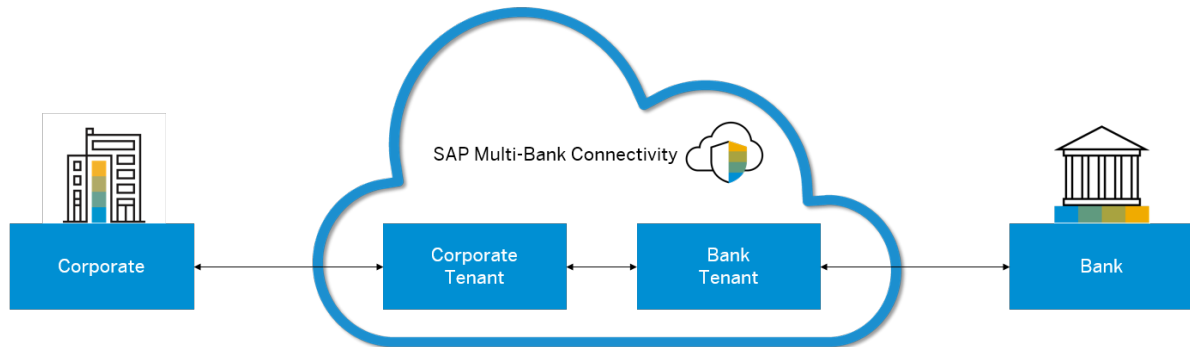
Banks can opt to join SAP Multi-Bank Connectivity as a member. In this case, they subscribe to the network to provide an easier and less complicated integration for corporate customers utilizing SAP Multi-Bank Connectivity.

They are provided with one test and one productive tenant in the SAP Multi-Bank Connectivity network much like a corporate customer. This provides multiple benefits, such as:

- Easier onboarding
- Dedicated bank support

- Reduced effort
- Faster kick off to go-live by utilizing a preconfigured connection to the bank

Subscription



If a member bank is on the list of banks the customer would like to onboard, the member bank onboarding is the default connection method. We always recommend prioritizing member banks for go-live in order to obtain value from SAP Multi-Bank Connectivity as quickly as possible.

Connecting Member Banks

Member banks can connect to SAP Multi-Bank Connectivity in several ways.

SFTP

SAP recommends a bank-hosted Secure File Transfer Protocol (SFTP) connectivity for message exchange as it provides simple and effective scalability options.

API

SAP Multi-Bank Connectivity also offers the possibility to enable the digital connection using banking API. After the banks specifications have been verified to meet the technical standards of the product, SAP Multi-Bank Connectivity adheres to the APIs provided by the member bank.

Note

For more information on current SAP Multi-Bank Connectivity member banks, speak to your SAP Multi-Bank Connectivity onboarding team.

1.1.2.3 EBICS

An EBICS contract with the bank is the prerequisite to leverage this type of integration. The customer needs to request the EBICS partner ID and user IDs.

Some of the common concepts regarding EBICS are explained in the following sections.

EBICS Users

Banks will usually provide the customer with two users. One of these needs to be maintained on the SAP Multi-Bank Connectivity side in order to open the connection to send and receive messages. A second user is usually maintained as a backup and sometimes the bank will require both users to open the connection.

Supported Versions

EBICS 2.5 (German standard) and EBICS 3.0 are currently supported with the signature mechanisms A005 and A006.

For more information on EBICS 3.0, see the corresponding [What's New](#) topic.

Note

SAP Multi-Bank Connectivity does not support storing certificates on hardware device, which is a requirement for the French EBICS TS protocol. For more information, please see **EBICS TS** in the glossary.

Related Information

[Glossary](#)

1.1.2.3.1 Onboarding Process and Initialization Process (INI and HIA)

Initial Communication

At this point, the bank must specify the order types and the BIC used by the customer. The customer and the bank need to decide on these two items – the SAP Multi-Bank Connectivity team has no input here.

User Initialization

Once the contract between the customer and the financial institution is concluded, a set of key pairs is generated per user on the customer's SAP Multi-Bank Connectivity tenant. The public keys for each user are then transmitted to the bank system by means of the EBICS administrative order types INI and HIA. After the successful processing of the INI and HIA orders, SAP Multi-Bank Connectivity generates INI and

HIA initialization letters that must be returned signed to the financial institution by the customer. This step is referred to as user initialization.

Download the Financial Institution's Public Keys

A successfully initialized user can download all public keys from the financial institution by means of a specially provided administrative order type (HPB). The processing of HPB requires a single EBICS request / response pair. The EBICS request of HPB contains the user's identification and authentication signature itself.

Points to Note

- To ensure the utmost security, all letters and certificates are created directly in the customer's SAP Multi-Bank Connectivity tenants and linked to the bank's URL – this ensures that the certs cannot be used by or with another system.
- Order types are a subcategory of message types and need to be correct or the bank will reject the file.
- Certificates generated for SAP Multi-Bank Connectivity are usually valid for two years.
- Most banks who connect with EBICS don't have a test environment. This means that payment testing (penny testing) can only be carried out in production. Here, it's best to send payments of a very small amount between bank accounts and notify the bank that these will be tests.
- If the INI and HIA letters are set up in the SAP Multi-Bank Connectivity test environment where there's no test system on the bank's side, they'll need to be reset by the bank, reissued by SAP Multi-Bank Connectivity, and resigned by the customer before they can be run in another system – that is, the production system.
- If it's detected that the current key is no longer valid, SAP Multi-Bank Connectivity automatically retrieves and updates the public key of the financial institution via an HPB order type.

1.1.2.3.2 Order Type Determination (EBICS 2.5)

Order types are a subcategory of message type. It's essential that these are defined correctly in order for the bank to accept the payment. This needs to be determined between the customer and the bank and relayed to the SAP Multi-Bank Connectivity onboarding team before the payments are sent. The rules for order type determination are defined in the source system (customer ERP). For more information on how to configure order types, see the related information on EBICS Order Type Determination.

Note

Order types are only relevant for EBICS version 2.5. With version 3.0, order types have been replaced by the Business Transaction Format (BTF) concept.

Related Information

[EBICS Order Type Determination](#)

1.1.2.3.3 BTF Concept (EBICS 3.0)

The Business Transaction Format (BTF) concept has been introduced in EBICS 3.0 to replace order types.

The BTF concept is currently only available with the connector for SAP Multi-Bank Connectivity. For detailed information, please follow the links below.

Related Information

[EBICS BTF Settings for connector for SAP Multi-Bank Connectivity \(BSNAGT\)](#)

1.1.2.3.4 EBICS User Determination

SAP Multi-Bank Connectivity recommends utilizing one or two static users for approval in the EBICS scenario. Upon request during onboarding, the EBICS users used to initiate the payment can be dynamically selected based on the users that approved the payments in SAP S/4HANA.

Related Information

[Static EBICS Users \(for SAP ECC\)](#)

[Static EBICS Users \(for S/4Hana\)](#)

[Maintain Static EBICS Users \(for S/4HANA Cloud\)](#)

1.1.2.3.5 Support of Hardware Security Modules

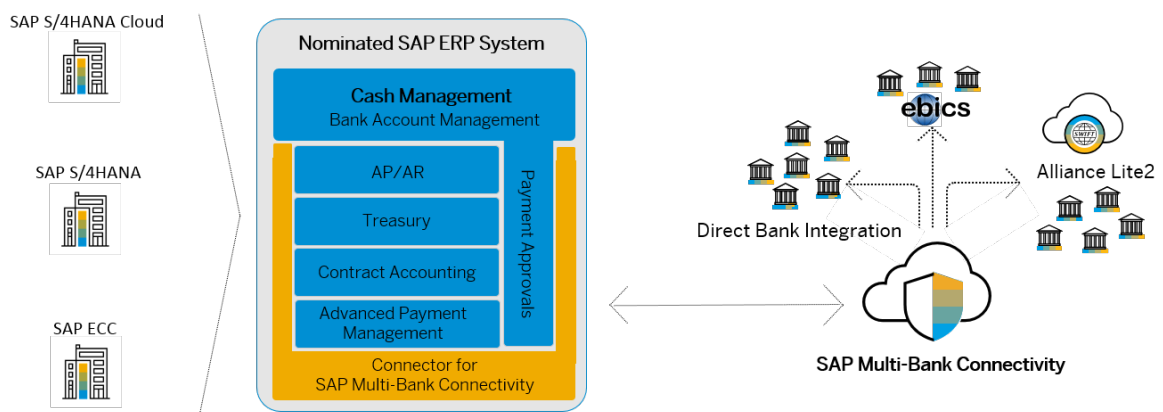
SAP Multi-Bank Connectivity does not support the use of certificates stored on hardware devices. This will prevent the use of the EBICS TS profile, which is specific to France.

1.1.2.4 Multiple ERP Systems and SAP Multi-Bank Connectivity

It's possible to connect multiple ERP systems to the cloud service. Unless agreed in the onboarding project, multiple systems can send messages, but only one system can receive messages, such as status notifications or account statements. For an optimized setup, SAP recommends leveraging SAP S/4HANA Finance for advanced payment management to centralize payments within an SAP S/4HANA system. Alternatively, customers can utilize the file pickup utility of the connector for SAP Multi-Bank Connectivity to pick up files from a shared location between the multiple systems and centralize at least the communication from one nominated ERP system.

The following image illustrates one nominated system for SAP Multi-Bank Connectivity integration and data exchange to banks:

Example: Multiple ERP Integration



1.1.2.5 Third-Party Tool Integrations

Some customers wish to use third-party solutions instead of a direct bank integration. In such cases, SAP can treat such a third-party product like a bank and integrate using an SFTP server of the third-party provider.

1.1.3 Service Consumption

Note

This applies only to production environments.

SAP Multi-Bank Connectivity customers are allowed a tiered amount of transactions.

The tiered amount of transactions is agreed in the commercial discussion between the customer and their SAP Account Executive during the sales process. The minimum transaction quantity to be subscribed to is one (1) block of 1,000 transactions.

As an SAP Multi-Bank Connectivity customer, if you want to discuss or review your subscription package in your managed cloud, including licenses, you'll need to contact your SAP Account Executive. The SAP Multi-Bank Connectivity onboarding or support team won't be able to advise you on the tiered amount of transactions that you're entitled to.

Once you're live in production, you can access your consumption via the [SAP for Me portal](#).

Note

For more information on SAP for Me, see the following resources:

- [SAP Support Portal: SAP for Me](#)
- [SAP for Me blog post](#)
- [SAP for Me Capability Map](#)
- [SAP for Me User Help](#)

1.2 Security Capabilities

To set up a secure connection between a customer system and SAP Multi-Bank Connectivity, several artifacts must be exchanged, such as public keys for Transport Layer Security (TLS) and Message Layer Security (MLS) encryption/decryption. In addition, it may be necessary to allowlist SAP IP ranges depending on your firewall position.

Message Level Security is optional for bank connections but highly recommended by SAP for the secure transfer of data. For bank connections, the artifacts required depend on connectivity options and security levels. For the customer to SAP Multi-Bank Connectivity portion, the use of Message Level Security is mandatory.

Note

Security artifacts will be required for your test and productive systems.

IP Allowlisting

Note

IP allowlisting is required, only where applicable, by SAP ECC customers, SAP S/4HANA customers, non-SAP ERP customers, and banks and third-party service providers using host-to-host connectivity types.

Corporate customers responsible for the maintenance of the above ERP types, banks, and third-party service providers reserve the right to decide whether IP allowlisting is mandatory for them or not.

To onboard to SAP Multi-Bank Connectivity, you may need to allowlist SAP hostnames and IP ranges for SFTP and Web service connections.

Allowlisting doesn't apply to customers using SAP S/4HANA Cloud, or where your bank or financial institution use EBICS and/or SWIFT. Only banks using host-to-host connectivity need to apply allowlisting rules, depending on their individual network/firewall configurations.

If you're using SFTP and your firewall is in front of the SFTP server, you must allowlist. To ensure smooth onboarding, please check with your network administrator if allowlisting is necessary, for instance, where your network configuration is maintained in-house and not by SAP. This is a mandatory requirement.

For a list of IP ranges, see [Regions and Hosts Available for the Neo Environment](#).

Transport Layer Security (TLS)

TLS is a cryptographic protocol designed to provide communication security over a network. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications, for example, between a client (bank system) and a server, such as the SAP Multi-Bank Connectivity tenant, or a customer ERP system and SAP Multi-Bank Connectivity tenant.

Note

The same security artifacts can't be used for your test and production environments. Using the same certificates for test and production poses a significant risk to the integrity and security of your connection to and subsequent data being exchanged with SAP Multi-Bank Connectivity.

As part of the onboarding process, banks will be asked to upload their test and production security artifacts. If your bank or financial institution can't provide these artifacts, they should provide the date when you agree to provide each of these artifacts to SAP.

Note

For further information on mandatory TLS requirements and trusted certificate authorities, see [Certificate Requirements and Trusted Certificate Authorities \[page 21\]](#).

SFTP Connections

SSH is the default authentication method for SFTP connections using the Push/Pull scenario described in [Host-to-Host \[page 13\]](#).

Non-SFTP Connections

For non-SFTP connections, your system must mutually authenticate using X.509/SSL certificates. SAP has a list of trusted certificate authorities that include the most common, globally recognized certificate authorities.

📘 Note

For SAP S/4HANA Cloud, private edition, SAP ECC customers, and all bank connections, please ensure that you have or procure different certificates for your TEST and PROD environments, that they're signed by a trusted SAP CA, and that they're valid for at least one year.

Message Layer Security (MLS)

MLS ensures the integrity and privacy of messages through encryption and signing using public and private keys. While TLS provides a secure channel for data to pass through, MLS provides an additional layer of security to message content. Message level security is mandatory for all customer to SAP Multi-Bank Connectivity connections in TEST and PROD environments and optional (but highly recommended) for all SAP Multi-Bank Connectivity to FSI connections.

When using MLS, please ensure that you have PKCS7 certificates for your TEST and PROD environments signed by one of our trusted certification authorities. For more information, see [Certificate Requirements and Trusted Certificate Authorities \[page 21\]](#).

Your bank or financial institution should ensure that these are available as soon as possible and that they're valid for at least two years. This will speed up the onboarding process.

📘 Note

MLS is optional for SAP Multi-Bank Connectivity to bank connectivity, but strongly recommended. However, if your bank or financial institution can't use or support MLS, they should inform the customer and the SAP Multi-Bank Connectivity Onboarding team explicitly as part of the onboarding process.

For more information, see [Regions and Hosts Available for the Neo Environment](#).

1.2.1 Certificate Requirements and Trusted Certificate Authorities

A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

In SAP Multi-Bank Connectivity, certificates must be signed by an SAP-trusted CA. In order to connect to SAP Multi-Bank Connectivity, all certificates used to establish transport level security need to be signed by an SAP-trusted certificate authority. Please note that only the certificate authorities listed in the following table are accepted by SAP Multi-Bank Connectivity.

📘 Note

For any connection to SAP Multi-Bank Connectivity, you'll need to have certificates signed by a CA – this is a mandatory security requirement.

Trusted CA	Serial Number	Valid From	Valid To
Amazon Root CA 1	14326697891665585687803 4712317230054538369994	2015.05.26	2038.01.17
Atos TrustedRoot 2011	6643877497813316402	2011.07.07	2030.12.31
Baltimore CyberTrust Root	33554617	2000.05.12	2025.05.12
certSIGN ROOT CA	35210227249154	2006.07.04	2031.07.04
Certum CA	65568	2002.06.11	2027.06.11
Certum CA	293460	2009.03.03	2024.03.03
COMODO Certification Authority	4339081803284281854063 5488309124489234	2011.01.01	2030.12.31
COMODO ECC Certification Authority	4157828386708669263825 6921589707938090	2008.03.06	2038.01.18
COMODO RSA Certification Authority	1019090845375820933089 41363524873193117	2010.01.19	2038.01.18
DigiCert Assured ID Root CA	171547179341205878621677 94914071425081	2006.11.10	2031.11.10
DigiCert Global Root CA	10944719598952040374951 832963794454346	2006.11.10	2031.11.10
DigiCert Global Root CA	8796353606545229494490 896265396764727	2013.03.08	2023.03.08
DigiCert Global Root G2	4293743540046975378534 879503202253541	2013.08.01	2038.01.15
DigiCert High Assurance EV Root CA	35534000764105479197247 30734378100087	2006.11.10	2031.11.10
DigiCert High Assurance EV Root CA	13785899061980321600472 330812886105915	2008.04.02	2022.04.03
DigiCert High Assurance EV Root CA	16582437038678467094619 379592629788035	2013.10.22	2028.10.22
Entrust Root Certification Authority	1164660820	2006.11.27	2026.11.27
Entrust Root Certification Authority	1372799044	2014.09.22	2024.09.23
Entrust Root Certification Authority - G2	1246989352	2009.07.07	2030.12.07
Entrust Root Certification Authority - G2	1372807406	2014.10.22	2024.10.23
Entrust.net Certification Authority (2048)	946069240	1999.12.24	2029.07.24
GeoTrust Global CA	144470	2002.05.21	2022.05.21
GeoTrust Primary Certification Authority - G2	80682863203381065782177 908751794619243	2007.11.05	2038.01.18

Trusted CA	Serial Number	Valid From	Valid To
GlobalSign ECC Root CA - R4	14367148294922964480859 022125800977897474	2012.11.13	2038.01.19
GlobalSign ECC Root CA - R4	1596622236128948842396 37590694	2012.11.13	2038.01.19
GlobalSign Root CA	4835703278459707669005 204	1998.09.01	2028.01.28
GlobalSign Root CA - R3	4835703278459759426209 954	2009.03.18	2029.03.18
GlobalSign Root CA - R6	14177666179734449892526 70301619537	2014.12.10	2034.12.10
GlobalSign Root R46	15526176884669505479588 67513931858518042577	2019.03.20	2046.03.20
Go Daddy Class 2 Certification Authority	0	2004.06.29	2034.06.29
Go Daddy Root Certificate Authority - G2	7	2011.05.03	2031.05.03
Go Daddy Root Certificate Authority - G2	0	2009.09.01	2037.12.31
GTS Root R1	146587175971765017618439 757810265552097	2016.06.22	2036.06.22
GTS Root R1	15966232030972641740417 8440727	2016.06.22	2036.06.22
GTS Root R2	14658717605576705381447 9386953112547951	2016.06.22	2036.06.22
GTS Root R2	1596624494066223497690 42896298	2016.06.22	2036.06.22
GTS Root R3	146587176140553309517047 991083707763997	2016.06.22	2036.06.22
GTS Root R3	15966249540113685270785 7743206	2016.06.22	2036.06.22
GTS Root R4	14658717622935043991651 9468929765261721	2016.06.22	2036.06.22
GTS Root R4	15966253270076021536894 2768210	2016.06.22	2036.06.22
ISRG Root X1	1728869286697904760646 70243504169061120	2015.06.04	2035.06.04
ISRG Root X2	87493402998870891108772 069816698636114	2020.09.04	2040.09.17
QuoVadis Root CA 2	1289	2006.11.24	2031.11.24
QuoVadis Root CA 2 G3	39015607945895925744613 3169266079962026824725 800	2012.01.12	2042.01.12

Trusted CA	Serial Number	Valid From	Valid To
Starfield Class 2 Certification Authority	0	2004.06.29	2034.06.29
Starfield Services Root Certificate Authority - G2	0	2009.09.01	2037.12.31
SwissSign Gold CA - G2	13492815561806991280	2006.10.25	2036.10.25
SwissSign Platinum CA - G2	5670595323396054351	2006.10.25	2036.10.25
SwissSign Silver CA - G2	5700383053117599563	2006.10.25	2036.10.25
TC TrustCenter Class 2 CA II	57424572311236023459850 9331795238	2009.11.03	2025.12.31
thawte Primary Root CA	2994832722786294443078 0750156152137111	2013.10.31	2023.10.30
T-TeleSec GlobalRoot Class 2	1	2008.10.01	2033.10.01
USERTrust RSA Certification Authority	26450937647810587875918 71645665788717	2010.02.01	2038.01.18
VeriSign Universal Root Certification Authority	14027290347807690984722 0679656918640734	2013.04.09	2023.04.08

Mandatory Requirements for TLS Certificates

To establish connectivity between a corporate ERP and their SAP Multi-Bank Connectivity tenants, you must use valid TLS certificates. This is a platform-level (SAP BTP) mandatory requirement, and every customer has to follow the same process of connecting to SAP Multi-Bank Connectivity. Consider the following points when procuring TLS certificates for use with SAP Multi-Bank Connectivity:

- The reason to use TLS:
TLS certificates enable an additional level of security to make sure that only authorized systems can send messages to SAP Multi-Bank Connectivity tenants.
- Data segregation:
You can't use wildcard or multiuse (one cert for TEST and PROD). By having separate certificates for TEST and PROD, we enable additional control to ensure that traffic between TEST ERP and PROD ERP are distinctly separated and secured by different certificates.
- Multiple ERPs in one certificate:
To reduce expenses for certificate signature with an external CA, you can have multiple test environments listed in one certificate. This is achieved by listing additional systems under Subject Alternative Names (SAN). This is only applicable to test instances, as customers generally use only one production ERP.
- Steps required to generate a signature request:
This is unique to each customer's setup and security protocols. There are different ways to generate a signature request, and we let the customer and/or implementation partner decide on the best approach. In most ERPs, there's an option in STRUST to generate a certificate signing request. Your Basis admin team can advise on the most suitable and effective means.

- Subject field in TLS certificate:
The best practice is to use each system's Fully Qualified Domain Name (FQDN) for the subject name or SAN. Additional information on how you can identify the FQDN of your system can be obtained from your Basis administrator.
- Validity of TLS certificates:
In line with CA/PKI industry practices and SAP's own Cryptographic Key Management policies, the maximum validity period allowed for a third-party CA-signed client certificate is 13 months (398 days). This applies to all PKI/TLS certificates used for authentication between a customer asset and an SAP Multi-Bank Connectivity asset and/or all contexts in which communication between customer-SAP Multi-Bank Connectivity assets is transmitted over the public Internet.

1.2.2 SAP Multi-Bank Connectivity Security Datasheet

SAP Multi-Bank Connectivity is an on-demand Software-as-a-Service (SaaS) solution that connects financial institutions and other financial service providers with their corporate customers over 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, SAP Multi-Bank Connectivity implements comprehensive security measures in the area of physical security, application 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 SAP Multi-Bank Connectivity.

Product Release

[What's New in SAP Multi-Bank Connectivity](#)

Terminology

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

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

1.2.2.1 SAP Multi-Bank Connectivity Cloud Scenario

The SAP Multi-Bank Connectivity cloud scenario follows the Outsourced Community Cloud scenario, the SaaS Provider/Consumer Scope of Control model, the push/pull model, and global distribution.

1.2.2.1.1 Outsourced Community Cloud Scenario

According to *NIST Cloud Computing Synopsis and Recommendations (special publication 800-146)*, SAP Multi-Bank Connectivity can be regarded as an *Outsourced Community Cloud*. Here the term *outsourced* means outsourced from the SAP Multi-Bank Connectivity customer perspective. In this scenario, SAP hosts the SAP Multi-Bank Connectivity service as a cloud solution. The SAP Multi-Bank Connectivity cloud solution is targeted at and can only be accessed 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.

1.2.2.1.2 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)*, SAP 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.

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

1.2.2.1.3 Push/Pull Model

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

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

1.2.2.1.4 Global Distribution

SAP Multi-Bank Connectivity is offered by the data centers in St. Leon-Rot and Frankfurt, Germany.

Details of Data Centers

Data Center	Data Center ID	SAP-Owned Data Center/Third-Party Data Center	SAP-Operated	SAP Multi-Bank Connectivity Use
St. Leon-Rot, Germany	RO2	SAP-owned data center		CPI SaaS tenants
Frankfurt, Germany	FR4	Colocation		CPI SaaS tenants
Amsterdam, Netherlands		Colocation		CPI SaaS tenants
Sydney, Australia	D10	Colocation		CPI SaaS tenants

ⓘ Note

Colocation means that SAP 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. SAP Multi-Bank Connectivity uses a floor-to-roof caged space in which all the equipment is owned, installed, and operated by SAP.

1.2.2.2 Technical Security

Technical security covers all security-related aspects of how data is protected by the framework during the execution of an SAP 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.

1.2.2.2.1 Identity Management and Permissions

Within the SAP network, each user (SAP employee and customer alike) is assigned an SAP user account with corresponding unique ID and is authenticated/authorized against the SAP ID Service.

Underpinning all SAP assets (except where additional/alternative mechanisms are employed), the SAP ID Service is the central service responsible for the management and administration of user identities/accounts and their respective lifecycles, from creation to deactivation.

Permissions, authorizations, and privileges are tied to this unique ID issued at the point of account creation (account enrollment due to employee hiring, promotion from contract employee to full-time employee, or customer account creation). As accounts are centrally managed and administrated, when a user leaves the company (volitional or otherwise), their account is immediately deactivated, after which point that ID will no longer be able to partake in, much less complete, an authorization check. All authorizations assigned to an ID, even if never unassigned, become invalid at the point of account deactivation.

Further to the management of the accounts lifecycle, the SAP ID Service is also responsible for enforcing the SAP Password Policy, wherein accounts recognized by the SAP ID Service must comply with core password requirements such as length, minimum/maximum validity, password reuse or history, and complexity.

SAP end-user access to internal assets is managed almost exclusively through an internal user and access management tool called Cloud Access Manager (CAM). CAM, much like the SAP ID Service, is a central companywide tool that allows for the packaging of variable levels of access to one or more assets into a single requestable profile. The access request is reviewed by a set of named approvers and either approved or rejected. These profiles also define a time period for which access is granted, which can range from 1 hour up to, but not exceeding, 6 months for productive assets. If access is not revoked manually by an approver, CAM will automatically revoke access once the validity period has elapsed. Users may request access again, but this will once again require review and approval.

From a connectivity standpoint within the SAP Multi-Bank Connectivity solution itself, incoming messages/requests are authenticated at **(a)** the load balancer level, corresponding to the region the tenant resides in, which checks the root certificate presented by the client against the configured list of trusted certificate authorities (CAs), and **(b)** permissions configured on each individual tenant. Failing the load balancer certificate check at (a) will halt the connection from proceeding further.

Access reviews (provisioning/deprovisioning) are mainly handled by the CAM tool, but manual access reviews are performed for specific assets in accordance with SAP Security Policies/ISO/SOC control requirements periodically.

SAP Multi-Bank Connectivity follows the SAP Accounts and Password standard for managing accounts and passwords. This standard establishes the minimum requirements for assigning, managing, and securing account passwords and passphrases for SAP IT systems and cloud services.

Multifactor authentication (MFA) provides an additional layer of security and can limit potential damage if credentials are lost or stolen. It acts as a safety net, providing a more comprehensive authentication process that helps to mitigate the human factor. A common example of MFA is the combination of a password with a one-time token or PIN provided through software on a smartphone, or via text message. Without both pieces of information, a user would not be able to gain access.

1.2.2.2 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. SAP Multi-Bank Connectivity uses SAP Adaptive Service Enterprise (ASE) for the main data storage, whereas the Business Cockpit uses the SAP HANA database. Data stored in SAP ASE 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 the SAP HANA database is encrypted using AES and a key length of 256 bits.

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's 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.

In general, SAP Multi-Bank Connectivity stores SAP Multi-Bank Connectivity messages for 90 days. SWIFT messages are stored for 124 days.

Backup and restore data is stored in secondary SAP data centers, for example, St. Leon-Rot being the secondary site for Frankfurt, and Frankfurt being the secondary site for St. Leon-Rot. Backup data is encrypted in transit and when stored in the secondary site.

1.2.2.3 Data Transmission and Data Flow Control

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

At the transport layer, connections in and out of SAP Multi-Bank Connectivity utilize Transport Layer Security (TLS) and Secure Shell (SSH). In line with industry-standard encryption protocol implementation practices, the Secure Sockets Layer (SSL) protocol is disabled in favor of TLS versions 1.2 or above, and the minimum bit length used for TLS/SSH asymmetric keys is 2048 bits. SAP supports TLS version 1.2 and above.

At the message layer, data encryption is mandatory. Message-layer encryption is achieved using various algorithms and key lengths. The available algorithms include AES/CBC. Strong encryption can be used for AES/CBC using a key length of 192 and 256 bits.

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

Use of X.509 Certificates and PGP Keys

HTTPS communication at the message entry of SAP Multi-Bank Connectivity is secured using PKI X.509 certificates. In line with standard PKI implementation, all HTTPS-based communication requires both client and server to possess and present a signed public certificate, obtained from a trusted third-party CA. Except for internal-only connectivity scenarios, wherein an explicitly DEV/QA asset (not including a Test/Staging asset) communicates with another DEV/QA asset, certificates signed by an internal CA are not allowed. For a complete list of currently supported CAs, see [Certificate Requirements and Trusted Certificate Authorities](#). Additional or heretofore untrusted CAs can be requested for inclusion on the SAP Multi-Bank Connectivity

Trusted CA List by a customer, barring the previously mentioned internally owned CAs, which would be rejected by default. Upon subsequent evaluation by both the central SAP Security team and later the SAP Multi-Bank Connectivity product team, a decision will be made on whether to add this CA to the Trusted CA List.

SAP Multi-Bank Connectivity uses the third-party certificate authority DigiCert for issuing certificates that represent parts of SAP Multi-Bank Connectivity.

Requirements for Cryptographic Keys

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

SAP Multi-Bank Connectivity recommends using public keys that are signed with minimum hashing standard SHA-2. SAP Multi-Bank Connectivity recommends that asymmetric keys are minimum 2048 bits long.

In line with internal SAP policies regarding the management and administration of cryptography material, all keypairs should have a validity period between but not exceeding 2–3 years (not including PKI X.509 keypairs where the maximum validity period is 13 months or 395 days), the signature algorithm of the keypair must be Secure Hashing Algorithm 2 (SHA-2) or above (the SHA-1 algorithm, while still used today, has been functionally broken since the early 2010s and will not be accepted), and the minimum key length for asymmetric keys is 2048 bits.

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 SAP 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 SAP 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 SAP 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 solution (PassVault) 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 SAP Multi-Bank Connectivity-hosted FTP server are stored securely in the file system of these components.

1.2.2.2.4 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 SAP Multi-Bank Connectivity license.
PROD	Standard prod cluster for customers who have purchased an SAP Multi-Bank Connectivity license.

In addition, SAP Multi-Bank Connectivity uses the following landscapes for internal purposes; these are also well isolated from each other.

Landscape	Purpose
VLAB	Dedicated for internal validation (outside DEV program). Test clusters of SAP Multi-Bank Connectivity Cloud Operations.
DEMO	Sales demo, customer demo by solution validation, and so on.

1.2.2.2.5 Cryptographic Algorithms Used by SAP Multi-Bank Connectivity

In its standard configuration, SAP 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		
	<ul style="list-style-type: none"> AES128-SHA256 AES256-SHA256 AES128-SHA AES256-SHA 	<ul style="list-style-type: none"> 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
	<ul style="list-style-type: none"> AES/CBC/ PKCs5Padding SHA512/RSA 	<ul style="list-style-type: none"> AES 	<ul style="list-style-type: none"> SHA512/RSA 	
Data at rest	n/a	SAP ASE <ul style="list-style-type: none"> AES128 HANA DB <ul style="list-style-type: none"> AES-256-CBC SFTP Server <ul style="list-style-type: none"> Same as data in transit/message layer Temporary files in file system RC4		
Data in processing (in memory)	n/a	No encryption/signing		
SIL – Data in transit	<ul style="list-style-type: none"> AES/CBC/ PKCs5Paddingkey length - 128 			

FIPS 140-2

SAP 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 SAP 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 SAP Note [2117112](#) (How to use the FIPS 140-2 certified Crypto Kernel with CommonCryptoLib).

1.2.2.2.6 Security by Component

Connector for SAP Multi-Bank Connectivity

The connector for SAP Multi-Bank Connectivity provides easy connectivity and integration to corporate customers when connecting to SAP Multi-Bank Connectivity. It can be installed in an SAP ERP system, such as SAP S/4HANA or SAP ECC, 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 underlying SAP ERP system, for example, SAP S/4HANA or SAP ECC. The connector provides encryption/decryption and signing/verification. The security key material used by the connector is stored in Personal Security Environments (PSEs). The security-related settings are administrated using transactions STRUST and SSFA.

1.2.2.3 User Interface Security

SAP Multi-Bank Connectivity Cloud Operations uses an Eclipse-based operations UI, in combination with UIs of SAP Business Technology Platform (SAP BTP).

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.

1.2.2.4 Layers of Information Security

1.2.2.4.1 Layer 1: Physical Site

SAP data centers are world-class data centers. The data centers in St. Leon-Rot and Frankfurt, Germany, and Sydney, Australia from where SAP Multi-Bank Connectivity is offered have 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 centers host 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).

1.2.2.4.2 Layer 2: Database

SAP Multi-Bank Connectivity stores its data in SAP Adaptive Server Enterprise (ASE), running in a high-availability setup as well as in the SAP HANA database. 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 St. Leon-Rot, Germany is backed up to Walldorf, Germany 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. An 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 2 hours. SAP's data backup and restore processes comprise regular backups on redundant media.

1.2.2.4.3 Layer 3: Middleware

SAP Multi-Bank Connectivity uses SAP Business Technology Platform (BTP) and SAP Integration Suite as platform and middleware, respectively.

SAP BTP supports multitenancy, 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.

1.2.2.4.4 Layer 4: Application

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

The runtime node performs SAP 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. SAP 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.

1.2.2.4.5 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 TippingPoint) detects potential intrusion attempts. A load balancer (vendor F5) terminates TLS and distributes the requests.

SAP 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.

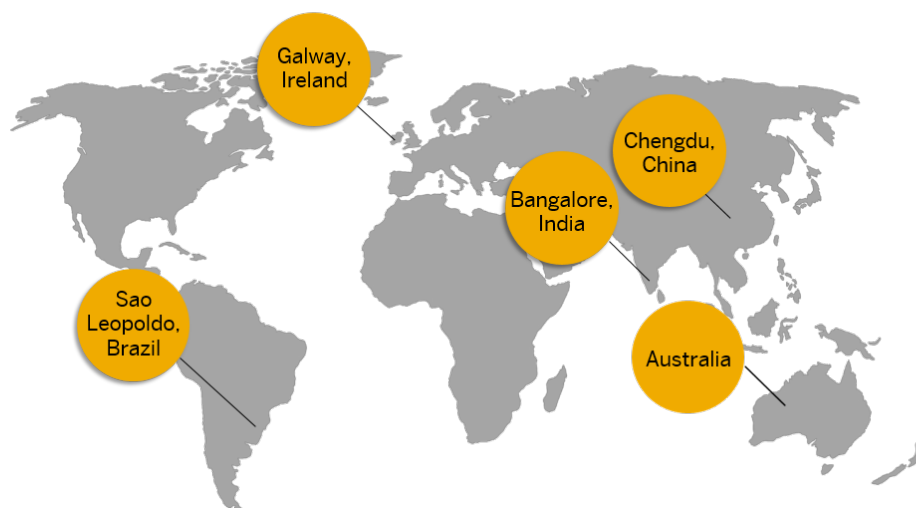
1.2.2.5 System Operations

SAP Multi-Bank Connectivity is operated by SAP Multi-Bank Connectivity Cloud Operations and supported by an SAP Multi-Bank Connectivity Support team within SAP. SAP Multi-Bank Connectivity Cloud Operations are on duty 24x7.

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.



Support established through a global network of SAP support hubs



1.2.2.5.1 Interaction with Customers

Interaction with customers is clearly defined along the following lines:

- **Onboarding:** For the onboarding of customers and banks up to the go-live of each bank connection, customer interaction is handled by the SAP Multi-Bank Connectivity Onboarding team. For more information, see [Onboarding Process](#).

- **Post go-live:** For post go-live support, such as technical support, maintenance activities, and so on, customer interaction is owned by the SAP Multi-Bank Connectivity Support and Operations teams. For more information, see [Support Information](#).

1.2.2.5.2 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.

1.2.2.5.3 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 Security Information and Event Management (SIEM) tool, Splunk, and operated by SAP. The system implements strict access control and log modification prevention. Audit logs are retained as per SAP standard. The load balancer as well as the intrusion prevention system also log in to the Splunk system.

1.2.2.6 Data Protection and Data Privacy

All data centers where the SAP Multi-Bank Connectivity solution is hosted are compliant with the relevant data protection and privacy laws.

Customer data processed by SAP Multi-Bank Connectivity is classified as confidential. Processing personal data is not part of the core functionality of SAP Multi-Bank Connectivity. SAP 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, an account number, is classified as sensitive personal data.

1.2.2.6.1 SAP Multi-Bank Connectivity as Data Processor

When a corporation or bank signs up to SAP Multi-Bank Connectivity and later exchanges payment instructions with SAP 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. SAP Multi-Bank Connectivity processes personal data and data in general on behalf of a corporation or bank and acts as data processor.

1.2.2.6.2 SAP Multi-Bank Connectivity as Data Controller

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

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

1.2.2.6.3 Third-Party Sub Processors for Personal Data

SAP Multi-Bank Connectivity maintains sub processor agreements with a set of third-party companies (non-SAP affiliates).

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

1.2.2.6.4 European General Data Protection Regulation

SAP Multi-Bank Connectivity is compliant with the European General Data Protection Regulation.

A dedicated European SAP Multi-Bank Connectivity Cloud Operations team handle the systems of European customers that contain encrypted data.

Personal data in SAP Multi-Bank Connectivity will only be accessible to these operators and not to operators outside of the European region.

1.2.2.7 Security Controls and Practices

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

1.2.2.7.1 Conclusion

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

1.2.2.7.2 Information Security Incident Management

Security incidents are handled according to the Security Incident Response and Management Standard.

The Security Incident Response and Management Standard is a framework designed to identify, investigate, and respond to potential security incidents to minimize the impact to SAP and to support rapid containment. The SAP incident response process follows the *NIST SP 800-61 Computer Security Incident Handling* guide, which provides the stages for the incident response lifecycle.

Vulnerability Assessments and Penetration Tests

Vulnerability assessments and penetration tests are executed regularly by the SAP internal team and third parties in request of SAP. Penetration tests focus on the network and infrastructure layer, whereas vulnerability assessments focus on SAP Multi-Bank Connectivity business functionality. Penetration test results are SAP confidential information and are generally not shared.

Virus Scanning

For data entry points (message entry, UI fields) virus scanning and in general, scanning against malicious content is implemented. On-access virus scanning for file system as well as regular full file system scanning is also implemented.

1.2.2.7.3 Security Education and Awareness

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

1.2.2.7.4 Compliance Standards

SAP Multi-Bank Connectivity is compliant with SAP-internal security policies, procedures, directives, guidelines, and product security standards. For more information, visit the [SAP Trust Center](#) and search for SAP Multi-Bank Connectivity.

1.2.2.7.5 Secure Software Development and Operations Lifecycle

The development of SAP Multi-Bank Connectivity follows the SAP Secure Software Development and Operations Lifecycle (Secure SDOL).

As part of this, regular quality gates need to be passed. Source code is scanned at a defined frequency for security issues using SAST/DAST tools and the outcomes are 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.

1.2.2.7.6 Export of Data in the Cloud

The customer can request the export of data since the data export functionality is mentioned in the contract between the customer and SAP. The customer may request the export of their own data (for example, transaction data, master data, configuration data) to an appropriate media and in an appropriate, understandable data format, such as CSV, PDF, or other standard machine-readable formats offered by SAP, for example, JSON or XML.

Note

This is not applicable for non-productive data.

1.2.2.7.7 Customer Data Deletion

During the tenant decommissioning process, customer data in the cloud environment is securely deleted as per the contractual obligation. The customer has the right to request for data deletion when they want to terminate the contract with SAP.

1.2.2.8 Further Information

SAP Multi-Bank Connectivity Solution Overview

[SAP Multi-Bank Connectivity product page](#) 

Certificate Authorities Supported by SAP Multi-Bank Connectivity

[Certificate Requirements and Trusted Certificate Authorities](#)

The Secure Software Development Lifecycle at SAP

[The Secure Software Development Lifecycle at SAP](#) 

Connector for SAP Multi-Bank Connectivity

[Connector for SAP Multi-Bank Connectivity - SAP Help Portal](#)

1.2.2.9 Contacts

For further details, see [Support Information](#).

1.3 Onboarding Process

Connection to SAP Multi-Bank Connectivity

SAP Multi-Bank Connectivity provides a number of different options to connect your ERP system to your banks or financial services institutions (FSIs). There are two connections that need to be setup when you get onboarded to SAP Multi-Bank Connectivity: the first from your ERP system to SAP Multi-Bank Connectivity, and the second from SAP Multi-Bank Connectivity to your banks or FSIs.

If you are interested in the more technical setup, please see the [Capabilities \[page 6\]](#) section in this guide.

Phased Approach of the Onboarding Process

Generally, the onboarding to SAP Multi-Bank Connectivity will always follow a phased approach to provide consistency and clarity throughout the whole process.

There are three primary phases during the onboarding process:

Scoping Phase

Preboarding Phase

Implementation Phase

- [#unique_4/unique_4_Connect_42_subsection-im1 \[page 41\]](#)
- [#unique_4/unique_4_Connect_42_subsection-im2 \[page 42\]](#)
- [#unique_4/unique_4_Connect_42_subsection-im3 \[page 42\]](#)

Scoping Phase

The Scoping phase will determine the first steps of your onboarding.

1. You will receive the **Scoping Questionnaire** as part of the high-level scoping process.
 2. You will reach out to the banks in scope to gather the required information based on the **Scoping Questionnaire**.
 3. The **Scoping Questionnaire** must be completed and returned via email to the MBC Scoping team under sap-mbc-scoping@sap.com.
- In the next phase, you will receive documentation and guidance based on the scoping information that you provided.

All communication with the MBC Scoping team during this phase is via email.

Preboarding Phase

The Preboarding phase is to ensure all information required is gathered to move the next phase of your onboarding.

1. You will receive the **Preboarding documentation** including Welcome Pack, Checklist, and Bank Connection (if applicable).
 2. You will reach out to the banks in scope and SWIFT (if applicable) to gather the required information based on the **Preboarding documentation**.
 3. Complete the **Preboarding documentation** and return everything via email to the MBC Onboarding team under sapmbconboarding@sap.com.
- The next phase will start as soon as someone from the MBC team is assigned to your Onboarding project team.

All communication with the MBC Onboarding team during this phase is via email.

Implementation Phase

The Implementation phase consist of three sub-phases: the technical, validation, and promotion phases. A dedicated Onboarding team consisting of the Customer Success Manager (CSM) and the Technical Integration Engineer (TIE) will be assigned to you to proceed with the implementation phase of the onboarding process.

1. You will receive an email from your dedicated Onboarding team with guidance and next actions.
2. Once the onboarding process is completed, the day-to-day handling is handed over to the SAP Product Support team. If any issues occur in the future, you can log a support case 24/7 via SAP for Me.

Communication during the onboarding process should be handled directly via your dedicated MBC Onboarding team.

Note

The implementation phase differs depending on your ERP system and the banks or financial service institutions you have in scope.

1.3.1 Roles and Responsibilities

Learn about the different roles and their responsibilities working together in an SAP Multi-Bank Connectivity onboarding project.

Your SAP Multi-Bank Connectivity license includes access to a managed onboarding service that guides you in completing all necessary tasks to configure the data exchange and the connection between your SAP ERP system and your financial institutions via SAP Multi-Bank Connectivity. As SAP Multi-Bank Connectivity customer, you also have some responsibilities and tasks to fulfill.

Role	Responsibility
Customer Success Manager (CSM)	<ul style="list-style-type: none"> Acts as the primary point of contact for topics related to the SAP Multi-Bank Connectivity phased onboarding project. A CSM will only be allocated after the To-Do & Checklist has been completed and returned by the customer and satisfies the minimum requirement to proceed with the technical phase.
Technical Integration Engineer (TIE)	<ul style="list-style-type: none"> Acts as contact on technical topics related to the SAP Multi-Bank Connectivity phased onboarding process. Configures MBC tenant and connection with the customer ERP and the banks. A TIE will only be allocated after the To-Do & Checklist has been completed and returned by the customer and satisfies the minimum requirement to proceed with the technical phase.
Customer	<ul style="list-style-type: none"> Reviews and completes the Preboarding phase according to the To-Do & Checklist attached to the Welcome Pack email. Owns the contractual discussions with the banks. The SAP Multi-Bank Connectivity onboarding team will not be involved in contractual discussions of any nature between corporate customers and their banks. Engages from a business and technical perspective. It is essential that the customers' teams must provide the required expertise to complete all technical configuration and tasks. Leads and drives the conversation and testing with the banks. An excellent coordination between the corporate customers and their banks is required to ensure timely responses and actions taken by teams from both the customer and bank side.
Customer Tenant Administrator (Tenant Owner)	<ul style="list-style-type: none"> Configures target systems for user provisioning. Adds new administrators in the administration console for identity authentication. Gives tenant access to the MBC Security Team.

1.3.2 Connection Setup During Onboarding

There are two connections that need to be setup when you get onboarded to SAP Multi-Bank Connectivity:

1. From your ERP system to SAP Multi-Bank Connectivity, see here: [SAP ERP System Connectivity to SAP Multi-Bank Connectivity \[page 44\]](#)
2. From SAP Multi-Bank Connectivity to your banks or financial service institutions (FSIs), see:

1. [SWIFT – New and Migration Customers Scenario \[page 47\]](#)
2. [H2H, EBICS, Member Bank Scenario \[page 45\]](#)

Depending on which connection type you use, the steps and responsible parties can differ.

1.3.2.1 SAP ERP System Connectivity to SAP Multi-Bank Connectivity

Customers can connect to SAP Multi-Bank Connectivity using a number of different SAP solutions and deployment options.

The connector for SAP Multi-Bank Connectivity is a module designed to interact with the cloud service to standardize the integration. The connector is independent of the technical connectivity from ERP to SAP Multi-Bank Connectivity. The configuration of the connector for SAP Multi-Bank Connectivity is not part of the onboarding service. However, customers can follow the configuration guides to connect to the cloud service.

SAP System Type	Connector Installation/Configuration/Activation Required	Ownership	Notes
SAP S/4HANA Cloud <ul style="list-style-type: none"> • Basic Configurations 	Activation	SAP	For the activation, you need to log an incident under component <code>XX-S4C-OPR-SRV</code> . For more information, please see Support Information [page 50] .
SAP S/4HANA Cloud, private edition <ul style="list-style-type: none"> • Basic configurations • Advanced configurations 	Configuration	Customer/Partner	The connector for SAP Multi-Bank Connectivity is available in the system and only needs to be configured using the configuration guides.
SAP S/4HANA <ul style="list-style-type: none"> • Basic configurations • Advanced configurations 	Configuration	Customer/Partner	The connector for SAP Multi-Bank Connectivity is available in the system and only needs to be configured using the configuration guides.
SAP ECC 6.0 <ul style="list-style-type: none"> • Basic configurations • Advanced configurations 	Installation	Customer/Partner	The connector for SAP Multi-Bank Connectivity needs to be installed and can be configured using the configuration guides.

Related Information

[Connector for SAP Multi-Bank Connectivity](#)

1.3.2.2 H2H, EBICS, Member Bank Scenario

When connecting your ERP system and your financial institutions via H2H or EBICS, or when your bank is already a member bank, there are specific tasks that need to be performed by you or other responsible parties when following the five onboarding phases.

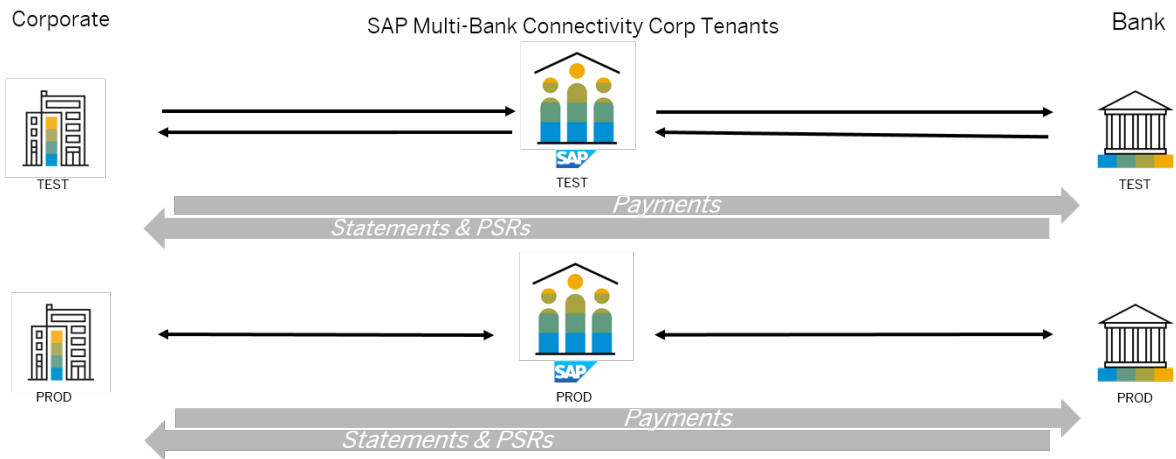
Phase 1: Preboarding	Tasks
Responsible parties: Customer, Bank	
1a Customer Preboarding	<p>Complete the To-Do & Checklist in either Corporate or Corporate S/4HANA Cloud tab and provide the information via email, which includes the following tasks:</p> <ul style="list-style-type: none">• Customer Tenant Owner to grant access to MBC Security officer• Installation and configuration of the connector for SAP Multi-Bank Connectivity (not applicable for S/4HANA Cloud)• Confirmation of completion of your ERP configuration
1b Bank Preboarding	<p>Complete the To-Do & Checklist in Banks Wave tab and provide the information via email, which includes the following tasks:</p> <ul style="list-style-type: none">• Discuss and agree with banks on connectivity type, file types and file formats• Align and agree Test timeframe and go-live date• Provide bank's connectivity details
Phase 2: Technical Integration	Tasks
Responsible parties: Customer, Bank, SAP	
2a Customer Technical Integration (not applicable for S/4HANA Cloud)	<ul style="list-style-type: none">• MBC onboarding Team (TIE):<ul style="list-style-type: none">• to confirm Customer Tenant access• to provide MBC Certificates (MLS & TLS)• to provide URL endpoints for RFC Destination configuration• Customer to run connectivity test (SAP ERP<>MBC)
2b Bank Technical Integration	<ul style="list-style-type: none">• MBC onboarding Team (TIE):<ul style="list-style-type: none">• to review bank connectivity details and perform connectivity test• to configure MBC tenant and advise of MBC readiness for E2E testing• Customer and bank align and confirm E2E test readiness
Phase 3: Customer Validation (Test)	Tasks
Responsible parties: Customer, Bank	

Phase 3: Customer Validation (Test) Tasks

Note
 As per MBC guidelines, maximum of 2 weeks per bank connection.
 MBC onboarding team is not required in bank's call with customer during this phase.

- Customer:
 - to coordinate with banks the testing plan and timeline and inform MBC onboarding team
 - to sign up for [Cloud System Notification Subscriptions \(CSNS\)](#) for platform maintenance and outage notifications
- Customer and banks to carry out E2E testing
- Customer to provide testing sign-off to MBC onboarding team

Demonstration of the SAP Multi-Bank Connectivity Landscape – Test Versus Production



Phase 4: Promotion (Production) Tasks

Responsible parties: Customer, Bank, SAP

Phase 4: Promotion (Production)**Tasks**

4a Customer Promotion (not applicable for S/4HANA Cloud)

- MBC onboarding team (TIE) to provide MBC Certificates (MLS & TLS)
- Customer
 - to proceed with installation and configuration of the connector for SAP Multi-Bank Connectivity on Production ERP
 - to confirm completion of production ERP configuration
 - to run connectivity test (SAP ERP<->MBC)
 - to advise MBC onboarding team (CSM) of the end users to be notified of SAP Product Support once the bank connections go live
 - to create S-user to enable SAP Product Support team to create support tickets on customer behalf. This is required so the support team can keep the customer proactively informed of any issues.
- SAP Product Support Team will provide the customer with a recording of the SAP MBC Support process via email along with additional documentation and KBAs.

4b Bank Promotion

- Customer to coordinate with banks the Penny testing plan, timeline, and inform MBC onboarding team
- MBC onboarding team (TIE)
 - to confirm availability for Penny test
 - to configure MBC tenant and provide MBC readiness for Penny test
- Customer and banks carry out Penny test
- Customer to provide Penny test sign-off

Phase 5: Support 24/7 (Production)**Tasks**

Responsible parties: Customer, SAP

- MBC onboarding team will handover connection to SAP Product Support team (24/7)
- Customer to create a ticket via Launchpad using the component LOD-FSN-SUP for any further assistance required with live connections, as they will be the customer's first point of contact.
- For formal escalation with live connections, please contact [Customer Interaction Center](#).

More information can be found here: [Support Information \[page 50\]](#)

1.3.2.3 SWIFT – New and Migration Customers Scenario

When connecting your ERP system and your financial institutions via SWIFT, there are specific tasks that need to be performed by you or other responsible parties when following the five onboarding phases.

Phase 1: Preboarding**Tasks**

Responsible parties: Customer, Bank, SWIFT

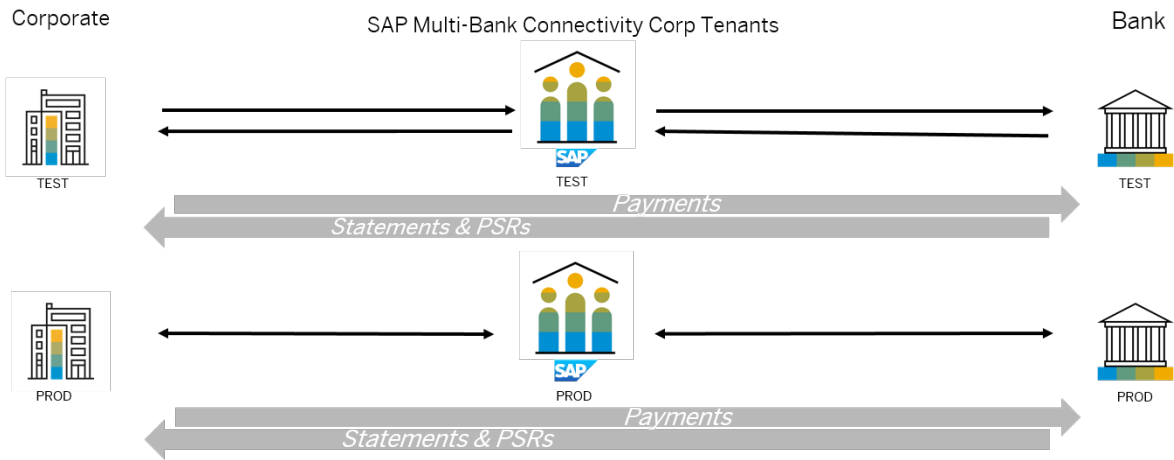
Phase 1: Preboarding	Tasks
1a Customer Preboarding	<p>Complete the To-Do & Checklist in either Corporate or Corporate S/4HANA Cloud tab and provide the information via email, which includes the following tasks:</p> <ul style="list-style-type: none"> • Customer Tenant Owner to grant access to MBC Security officer • Installation and configuration of the connector for SAP Multi-Bank Connectivity (not applicable for S/4HANA Cloud) • Confirmation of completion of your ERP configuration
1b Bank Preboarding	<ul style="list-style-type: none"> • Discuss and agree with banks on payment service and file formats • Complete To-Do & Checklist and provide information via email
1c SWIFT Preboarding	<ul style="list-style-type: none"> • Customer and SWIFT to start SWIFT onboarding process • Customer to trigger SWIFT CSP attestation and inform MBC onboarding team (mandatory step in SWIFT process to be completed prior to move to production) • Customer and SWIFT to decide on date of customer's BIC customization/nesting with SAP BIC
Phase 2: Technical Integration	Tasks
Responsible parties: Customer, Bank, SAP	
2a Customer Technical Integration (not applicable for S/4HANA Cloud)	<ul style="list-style-type: none"> • MBC onboarding Team (TIE): <ul style="list-style-type: none"> • to confirm Customer Tenant access • to provide MBC Certificates (MLS & TLS) • to provide URL endpoints for RFC Destination configuration • Customer to run connectivity test (SAP ERP<>MBC)
2b SWIFT Technical Integration	<ul style="list-style-type: none"> • MBC onboarding Team (TIE): <ul style="list-style-type: none"> • to confirm connectivity test (MBC<>SWIFT) • to configure MBC tenant and advise of MBC readiness for E2E testing • Customer and bank align and confirm E2E test readiness
Phase 3: Customer Validation (Test)	Tasks
Responsible parties: Customer, Bank	

Phase 3: Customer Validation (Test) Tasks

Note
 As per MBC guidelines, maximum of 2 weeks per bank connection.
 MBC onboarding team is not required in bank's call with customer during this phase.

- Customer:
 - to coordinate with banks the testing plan and timeline and inform MBC onboarding team
 - to sign up for [Cloud System Notification Subscriptions \(CSNS\)](#) for platform maintenance and outage notifications
- Customer and banks to carry out E2E testing
- Customer to provide testing sign-off to MBC onboarding team
- Customer to confirm completion of SWIFT CSP Attestation (mandatory step in SWIFT to be completed prior to move to production)

Demonstration of the SAP Multi-Bank Connectivity Landscape – Test Versus Production



Phase 4: Promotion (Production) Tasks

Responsible parties: Customer, SWIFT, SAP

Phase 4: Promotion (Production)	Tasks
4a Customer Promotion (not applicable for S/4HANA Cloud)	<ul style="list-style-type: none"> MBC onboarding team (TIE) to provide MBC Certificates (MLS & TLS) Customer <ul style="list-style-type: none"> to proceed with installation and configuration of the connector for SAP Multi-Bank Connectivity on Production ERP to confirm completion of production ERP configuration to run connectivity test (SAP ERP<->MBC) to advise MBC onboarding team (CSM) of the end users to be notified of SAP Product Support once the bank connections go live to create S-user to enable SAP Product Support team to create support tickets on customer behalf. This is required so the support team can keep the customer proactively informed of any issues. SAP Product Support Team will provide the customer with a recording of the SAP MBC Support process via email along with additional documentation and KBAs.
4b SWIFT Promotion	Customer to confirm with SWIFT team the date BIC will be available in production for Penny test and inform MBC onboarding team
4c Bank Promotion	<ul style="list-style-type: none"> Customer to coordinate with banks the Penny testing plan, timeline, and inform MBC onboarding team MBC onboarding team (TIE) <ul style="list-style-type: none"> to confirm availability for Penny test to configure MBC tenant and provide MBC readiness for Penny test Customer and banks carry out Penny test Customer to provide Penny test sign-off

Phase 5: Support 24/7 (Production)	Tasks
Responsible parties: Customer, SAP	
	<ul style="list-style-type: none"> MBC onboarding team will handover connection to SAP Product Support team (24/7) Customer to create a ticket via Launchpad using the component LOD-FSN-SUP for any further assistance required with live connections, as they will be the customer's first point of contact. For formal escalation with live connections, please contact Customer Interaction Center. <p>More information can be found here: Support Information [page 50]</p>

1.4 Support Information

If you require any support or have queries, you can contact the MBC support teams via ticket. They are located in Ireland, Belarus, Brazil, and the APJ region.

- Create a case 24/7 on [SAP for Me](#):

Component	Use in case of
LOD-FSN-SUP	Productive issues
LOD-FSN-INT	Non-productive or test system issues
LOD-FSN-CER	Certificate-related issues
	<p>Note</p> <p>The MBC team will reach out to you regarding expiring MBC certificates on your tenant side only. Please reach out to inform us via support ticket in case your third-party financial institution informs you of any upcoming changes on their side, for example, expiring public PGP key.</p>
LOD-FSN-REQ	For existing customers to initiate the onboarding process of additional banks via SAP Multi-Bank Connectivity. The component is not applicable to Swift-only customers.
	<p>Note</p> <p>Please give details of the bank, connectivity type, and timeline as agreed with your bank. Your ticket will be routed to the SAP Multi-Bank Connectivity onboarding team who will get in contact with you.</p>
LOD-FSN-AGT	Issues with connector for SAP for Multi-Bank Connectivity
XX-SER-SAPSMP-SUP	S-user issues or issues when subscribing to get Cloud Alert Notifications via the Cloud Availability Center
LOD-FSN-PAR	oOEM partner support
BC-NEO-CIS	Change or replacement of the tenant owner

- To receive availability notifications, sign up at [Cloud System Notification Subscriptions](#)

Note

To sign up for notifications, an S-user ID is required.

If you need more information on creating a ticket or S-user, please have a look at the following KBAs:

SAP Note	Title
1296527	How to create a support case (contact SAP Product Support)
1522544	How to change the priority of a support case
1271482	How does an administrator create or delete S-user IDs

Related Information

[SAP for Me](#)

[Notifications via S-User ID \[page 52\]](#)

1.4.1 Notifications via S-User ID

Find all information on S-user IDs and how to reach out if issues occur with it.

The support team communicates with customers

- via **support case** to inform about spikes in monitoring or expiring certificates for a specific customer
- via **Cloud Availability Center (CAC)** regarding central outages, maintenance activities and other topics that affect all customers

For these communication channels, an S-user ID is required. It is very important to sign up for S-users once your onboarding project moves to production to receive such notifications from SAP. Only an individual person can sign up for an S-user but you can have multiple S-users in place.

Cloud Availability Center

The Cloud Availability Center (CAC) gives you a personalized view into your SAP cloud products with status and availability, an events calendar, notifications history, and the latest news.

The application can be accessed via SAP for Me. You can access the current CAC user guide via the [Support Page](#).

Cloud Service Availability Notifications

The Cloud Service Availability Notifications allows you to manage subscriptions to CAC notifications related to issues that may impact your testing and subsequent go lives, as well as productive issues.

📌 Important

Find all information on how to set or remove the cloud notifications in the SAP Note [2900069](#).

Issues with S-User

If you have any issues with your S-user or subscribing to get notifications via the [Cloud Availability Center](#), create a case on SAP for Me using the `XX-SER-SAPSMP-SUP` component.

You can consult the following KBAs to learn more about S-users:

SAP Note	Title
2587408	S-user ID authorizations
2900069	How S-users can manage their own Cloud System Notification Subscriptions
1511008	How to add or change S-user ID authorizations
1282854	Information on adding/editing/deleting authorizations for S-user IDs
3108466	How to update S-user ID e-mail address
1271482	How does an administrator create or delete S-user IDs

Related Information

[SAP for Me](#)

[Users & Authorizations in SAP for Me](#)

[Contact the Customer Interaction Center](#)

1.4.2 Roles and Responsibilities in Support or Incident Case

Role	Responsibility
Customer	<ul style="list-style-type: none">• Reports incidents only through SAP for Me. <div data-bbox="850 510 1396 869"><p>📘 Recommendation</p><p>If you see any upcoming activities within your third-party ecosystem which are not directly addressable or monitored by SAP Multi-Bank Connectivity but may have a potential impact on the product's connectivity, please log a precautionary incident under LOD-FSN-SUP. Examples include (but are not limited to) the change of PGP keys on the bank side or an update of your EBICS certificate.</p></div> <ul style="list-style-type: none">• Cooperates with SAP Support to resolve incidents.• Provides email and phone details of customer contacts who SAP Support can contact at any time.• Provides adequate technical expertise and knowledge to enable SAP Support to reproduce, troubleshoot, and resolve issues.• Proactively logs support ticket if third-party certificates expire. See Support Information [page 50].• Regarding PGP renewal: organizes calls with bank and SAP Multi-Bank Connectivity support team
SAP 24x7 Support	<ul style="list-style-type: none">• Monitors the SAP support queue for new incident reports or incidents without processor.• Dispatches incidents to SAP Product Support or SAP Operations Support for root cause analysis and resolution.• Reproduces issue and perform root cause analysis.• Performs code-fixes, code reviews, regression tests, and deployment of fixes.• Creates SAP Knowledge Base Articles (KBAs) and SAP Notes.
SAP Multi-Bank Connectivity Support Team	<ul style="list-style-type: none">• Informs customer via ticket about upcoming certificate renewals on their tenants• Sets up a ticket and a subsequent call to rectify. <div data-bbox="850 1787 1396 1937"><p>📘 Note</p><p>Please be sure to have all accesses ready before the call.</p></div>

Related Information

[SAP for Me](#)

[Support Information \[page 50\]](#)

1.4.3 Escalation Path

If you want to escalate an existing incident, complete the following steps:

1. Call the [Customer Interaction Center \(CIC\) hotline](#).
2. Provide the CIC with the following information:
 - Incident number and priority
 - Date the incident was reported
 - Business impact of the incident

Note

The incident must qualify as a very high or high priority if being logged for an escalation via CIC.

CIC will create a Critical Incident Request, which is dealt with by the Critical Incident Management (CIM) team. The CIM team drive the escalation and assess the next steps.

Have a look at the following two KBAs for further information on changing priorities of a ticket and the general escalation process:



SAP Note	Title
1522544	How to change the priority of a support case - SAP for Me
90835	SAP Case Escalation Procedure

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 an 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.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

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

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.