CUSTOMER
SAP Multi-Bank Connectivity
2021-09-21

Security Datasheet

THE BEST RUN SAP

Content

1 SAP Multi-Bank Connectivity Security Datasheet. 4

1.1 The SAP Multi-Bank Connectivity Cloud Scenario. 4

Outsourced Community Cloud Scenario. 4

SaaS Provider/Consumer Scope of Control. 5

Push/Pull Model. 5

Global Distribution. 5

1.2 Technical Security. 6

Identity Management and Permissions. 6

Data Storage and Location. 7

Data Transmission and Data Flow Control. 7

Isolation and Multitenancy. 9

Cryptographic Algorithms Used by Multi-Bank Connectivity. 9

Security by Component. 10

1.3 User Interface Security. 11

1.4 Layers of Information Security. 11

Layer 1: Physical Site. 11

Layer 2: Database. 11

Layer 3: Middleware. 12

Layer 4: Application. 12

Layer 5: Network and Communication. 12

1.5 System Operations. 12

Permissions of Operators. 13

Interaction with Customers. 13

System Changes. 13

Handling of Cartridges. 13

Audit Logging. 13

Periodic Checks. 14

1.6 Data Protection and Data Privacy. 14

Multi-Bank Connectivity as Data Processor. 14

Multi-Bank Connectivity as Data Controller. 14

Third-Party Subprocessors for Personal Data. 15

Upcoming European General Data Protection Regulation. 15

1.7 Security Controls and Practices. 15

Conclusion. 15

Information Security Incident Management. 15

Consistently proven Security Measures. 16

Security Education and Awareness. 16
Compliance Standards. 16
Secure Software Development. 16
Reports that can be provided to Customers. 17
1.8 Disclaimer. 17
1.9 Further Information. 17
1.10 Contacts. 18

1 SAP Multi-Bank Connectivity Security Datasheet

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

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

For more details, see the additional information available on 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 *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.

1.1 The SAP Multi-Bank Connectivity Cloud Scenario

1.1.1 Outsourced Community Cloud Scenario

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

1.1.2 SaaS Provider/Consumer Scope of Control

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

Provider Control

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

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

1.1.3 Push/Pull Model

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

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

1.1.4 Global Distribution

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

Details of Data Centers

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

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

1.2 Technical Security

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

1.2.1 Identity Management and Permissions

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

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

Access to all functions, whether invoked manually by dialog users or automatically (for example, by a scheduler), is protected by a permission check. Multi-Bank Connectivity maintains a fine-grained permission concept. Fine-grained permissions are grouped and assigned to different personas such an SaaS administrator (Software-as-Service administrator) or tenant administrator. All permission assignments are tenant-specific, except for the SaaS administrator, who has broader permissions.

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

1.2.2 Data Storage and Location

All customer data at rest is stored encrypted.

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

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

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

1.2.3 Data Transmission and Data Flow Control

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

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

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

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

Use of X.509 Certificates and PGP Keys

HTTPS communication at the message entry of Multi-Bank Connectivity is secured using X.509 client certificates. Some of the Certificate Authorities (CAs) that are currently supported are *TC TrustCenter CA* and *Verisign Class3 Public Primary certificate Authority - G5*. For a complete list of currently supported CAs, see the link in chapter Further Information [page 17]. Additional CAs can be added on customer demand and after evaluation by the Multi-Bank Connectivity security team. Certificates are also used in various other use cases, such as digital signatures.

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

Requirements for Cryptographic Keys

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

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

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

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

Handling of Cryptographic Keys

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

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

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

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

1.2.4 Isolation and Multitenancy

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

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

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

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

1.2.5 Cryptographic Algorithms Used by Multi-Bank Connectivity

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

Data Lifecycle	Layer	Encryption/Signing Means		
Data in transit	Transport Layer	TLS	SSH	
		• AES128-SHA256 • AES256-SHA256 • AES128-SHA • AES256-SHA	• BLOWFISH-CBC • 3DES-CBC • AES128-CBC • AES128-CTR • AES192-CBC • AES192-CTR • AES256-CBC • AES256-CTR • ARCFOUR128 • ARCFOUR256 • CAST128-CBC • TWOFISH128-CBC • TWOFISH192-CBC • TWOFISH256-CBC	
	Message Layer	PKCS#7	PGP	XML Digital Signature

Data Lifecycle	Layer	Encryption/Signing Means
		• AES/CBC/ PKCs5Padding • SHA512/RSA • AES/ ZLIB • SHA512/RSA
Data at rest	n/a	Sybase • AES128 HANA DB • AES-256-CBC SFTP Server • Same as data in transit/ message layer Temporary files in file system RC4
Data in processing (in memory)	n/a	No encryption/signing

FIPS 140-2

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

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

1.2.6 Security by Component

Connector for the SAP Multi-Bank Connectivity

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

1.3 User Interface Security

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

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

1.4 Layers of Information Security

1.4.1 Layer 1: Physical Site

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

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

1.4.2 Layer 2: Database

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

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

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

Related Information

Data Storage and Location [page 7]

1.4.3 Layer 3: Middleware

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

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

1.4.4 Layer 4: Application

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

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

1.4.5 Layer 5: Network and Communication

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

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

1.5 System Operations

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

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

1.5.1 Permissions of Operators

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

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

1.5.2 Interaction with Customers

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

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

1.5.3 System Changes

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

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

1.5.4 Handling of Cartridges

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

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

1.5.5 Audit Logging

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

The audit log contains entries for configuration changes and security events, such as failed authentications. The audit log is stored in a third party audit log system (vendor Splunk) operated by SAP. The system

implements strict access control and log modification prevention. Audit logs are retained for 18 months. Audit logs can be provided to the customer on request. The load balancer as well as the intrusion prevention system also log in to Splunk.

1.5.6 Periodic Checks

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

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

1.6 Data Protection and Data Privacy

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

Customer data processed by Multi-Bank Connectivity is classified as confidential. Processing personal data is not part of the core functionality of Multi-Bank Connectivity. Multi-Bank Connectivity can however receive personal data as part of payment instructions. An example is a payment instruction sent by a corporation to a bank, where the payment beneficiary is a natural person. A part of the personal data, for example, account numbers, are classified as sensitive personal data.

1.6.1 Multi-Bank Connectivity as Data Processor

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

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

1.6.2 Multi-Bank Connectivity as Data Controller

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

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

1.6.3 Third-Party Subprocessors for Personal Data

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

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

1.6.4 Upcoming European General Data Protection Regulation

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

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

1.7 Security Controls and Practices

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

1.7.1 Conclusion

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

1.7.2 Information Security Incident Management

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

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

1.7.3 Consistently proven Security Measures

Vulnerability Assessments and Penetration Tests

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

Virus Scanning

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

1.7.4 Security Education and Awareness

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

1.7.5 Compliance Standards

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

1.7.6 Secure Software Development

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

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

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

1.7.7 Reports that can be provided to Customers

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

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

1.8 Disclaimer

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

1.9 Further Information

SAP Multi-Bank Connectivity Solution Overview

SAP Multi-Bank Connectivity product page

Certificate Authorities Supported by SAP Multi-Bank Connectivity

List of Trusted Certificate Authorities

SAP Security Development Lifecycle

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

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

Connector for the SAP Multi-Bank Connectivity

https://help.sap.com/mbc

1.10 Contacts

Multi-Bank Connectivity Solution Management

Multi-Bank Connectivity Marketing

Important Disclaimers and Legal Information

Hyperlinks

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

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

Videos Hosted on External Platforms

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

Beta and Other Experimental Features

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

Example Code

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

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.

www.sap.com/contactsap

THE BEST RUN SAP