Preboarding Guide
SAP Multi-Bank Connectivity

CUSTOMER

Date: 22-Oct-2019

Preboarding Guide

SAP Multi-Bank Connectivity

Typographic Conventions

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

Document History

Version	Status	Date	Change
1.0	Released to Customer	16-May-2019	Initial Release
1.1	Released to Customer	07-Aug-2019	EBICS section added
1.2	Final	22-Oct-2019	IP Range replaced with link to Help page.

Contents

1 About This Document

This document provides information for Financial Institutions who are onboarding to the SAP Multi-Bank Connectivity (MBC). To onboard to MBC, a number of preparatory steps are necessary. This document describes the necessary preparation prior to receiving the onboarding questionnaire which is vital to using MBC.

1.1 Target Audience

This document is for the technical implementation team involved in integration and onboarding, including potentially:

- Implementation and integration teams
- System Administrators
- Information Security Officers
- Network Administrators

2 Introduction

2.1 About MBC

SAP Multi-Bank Connectivity is an innovative solution that connects banks and other Financial institutions with their Corporate Customers on a secure network owned and managed by SAP. When interacting with MBC, corporate customers send payment instructions to MBC. Banks in turn send transaction status information and account reports back to the Corporate customer.

SAP Multi-Bank Connectivity combines SAP expertise in applications, analytics, and in-memory computing to provide a standard, on-demand innovative technology for financial institutions and their corporate customers on a platform that accommodates future integration needs.

Related Documentation

- SAP Multi-Bank Connectivity Product Page
- SAP Multi-Bank Connectivity Help

2.2 Online Onboarding Questionnaire

You will soon receive a link to an online questionnaire which is a mandatory step for onboarding to MBC. Providing SAP with a fully completed onboarding questionnaire makes it possible for all partners to onboard efficiently and effectively.
The sections which follow provide information and guidance for completing the onboarding questionnaire.

The questionnaire includes the following main sections:

- Your organization and team details
- Connectivity
- Messages

3 Organization

SAP recommends that one person coordinates all relevant parties needed to complete this questionnaire. The first portion of the questionnaire is related to organizational information in relation to your bank.

3.1 Bank Details

The following information is required:

- Bank Address
- Bank identification Code (BIC) - Please provide the BIC for your organization relevant to the integration for your corporate customers through MBC.

3.2 Your Onboarding Team

Onboarding to MBC requires SAP to determine technical information to build connectivity to SAP MBC. Therefore it is essential to compose your onboarding team accordingly. Assembling the members of your team is very important.

In some cases, all or some of these roles may be performed by the same person.

Roles include:

- Project Lead - Keeps the integration project running smoothly from start to finish
- Security & Network Lead –Provide technical information in relation to connection and encryption methods used by the bank. This person may be responsible for certificate and key procurement, along with IP and host whitelisting.
- Messaging Expert – Assist with messaging formats used. Advise on standards, regulations and special message formats used.
- Support Lead – Key point of contact for support issues post go live – Once the connection is activated, the support contact will assist with any issues.
- Technical Lead – Provides the expertise and task delegation from an integration point of view - the link between the various technical teams

You will be asked to state if you have previously performed B2B or Cloud integrations in the past. If yes, please state how many you have completed.

3.3 Corporate Connection

If your organization has corporate customer IDs to uniquely identify your customers, please provide SAP with this ID.

3.4 Environments

You need a Test and Production environment during the onboarding process.
In the questionnaire, please confirm that you have a test and a production environment for integrating to MBC.
The test system is used to simulate and test Connectivity, Validation and File Transmission.
Once testing has completed for all applicable scenarios, the production system will be activated.

4 Connecting Host to Host or Subscription

Two connection options are available when setting up a connection to MBC, Host to Host and Subscription.

Both have benefits.

A Host to Host connection sends messages from the Corporate system to the Corporate Tenant and then to a Bank back end system.

A subscription means that a Bank has its own Bank Tenant. This means that messages are exchanged using this tenant. If a bank has a number of corporate connections, this is the best option as it reduces the amount of direct connections from multiple Corporates.

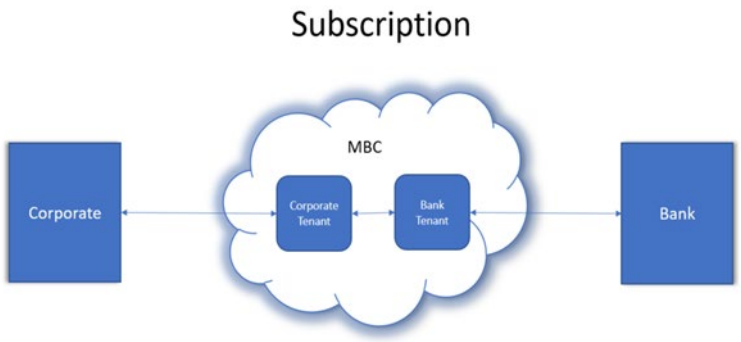
Subscription

As part of your subscription, you will be provided with one test and one productive tenant in the MBC network.

Please note that when a tenant is provided as part of your MBC subscription, there will be an S-user assigned to your tenant. The SAP MBC team requires this user number and user name to enable access to your tenant for the MBC onboarding team. Please provide the S-user ID for your tenants.

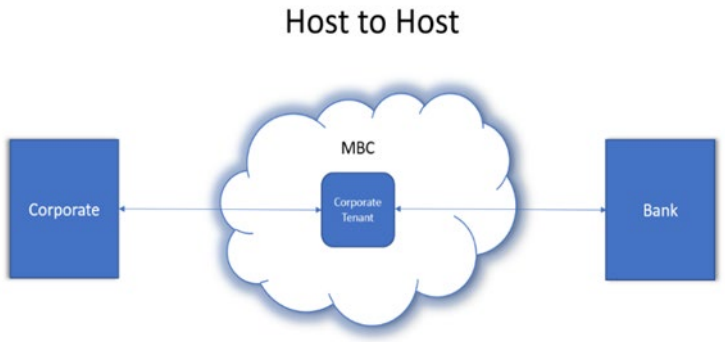
S-user – When a subscription is first signed, an S-user is assigned to the test and productive tenants. This S-user usually equates to the same person who signs the contract. It is important for you to determine who the S-user is in your organization and determine if that person wishes to continue as the administrator for your organization. SAP recommends that this S-user be one of your Technical leads.

More information on S-User can be found here.



Host to Host

Host-to-host (H2H) is an automated solution for high volume data transfer between banks and their corporate clients. In a Host to Host scenario, your organization is connected directly to the corporate customer's tenant in MBC.



4.1 EBICS

The Electronic Banking Internet Communication Standard (EBICS) Adapter allows SAP MBC and Corporates to communicate with banks using the EBICS protocol. For more information visit the EBIC's webpage.

5 Connection Methods

MBC offers the following connection methods:

- SFTP Push/Pull SSH
- AS2
- SOAP

For banks, SAP recommends self-hosted connectivity SFTP for message exchange as it provides simple and effective scalability options.

5.1 SFTP - Recommended

Secure File Transfer Protocol (SFTP) is a protocol that provides file access, file transfer, and file management over any reliable data stream. SFTP using secure Shell (SSH) is a cryptographic network protocol for operating network services securely over a network.

5.2 Webservices

SAP also offers connectivity using SOAP and AS2.

5.2.1 SOAP

Simple Object Access Protocol (SOAP) is a protocol designed to exchange information in the form of Web Services. It is primarily based on XML documents exchanged over HTTP.

SOAP web services are generally based on a Web Services Description Language (WSDL), which is an XML contract that defines the data and services offered by a given web service. The client and the server use this contract for exchanging information and making remote procedural calls.

If you choose SOAP in the MBC questionnaire, you will be requested to provide an endpoint for your test and production environments.

5.2.2 AS2

AS2 is a direct point to point connection. Messages are transmitted securely using HTTP and S/MIME.

If you choose AS2 in the MBC questionnaire, you will be requested to provide:

- Endpoints for your test and production environments
- AS2 IDs for your test and production environments

5.3 Communication Patterns

SAP MBC supports two communication patterns:

- Push/Pull
- Push/Push

This section outlines the communication patterns and use cases.

5.3.1 Push/Pull - Default for SFTP

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

Example:

SFTP sever is on Bank's side

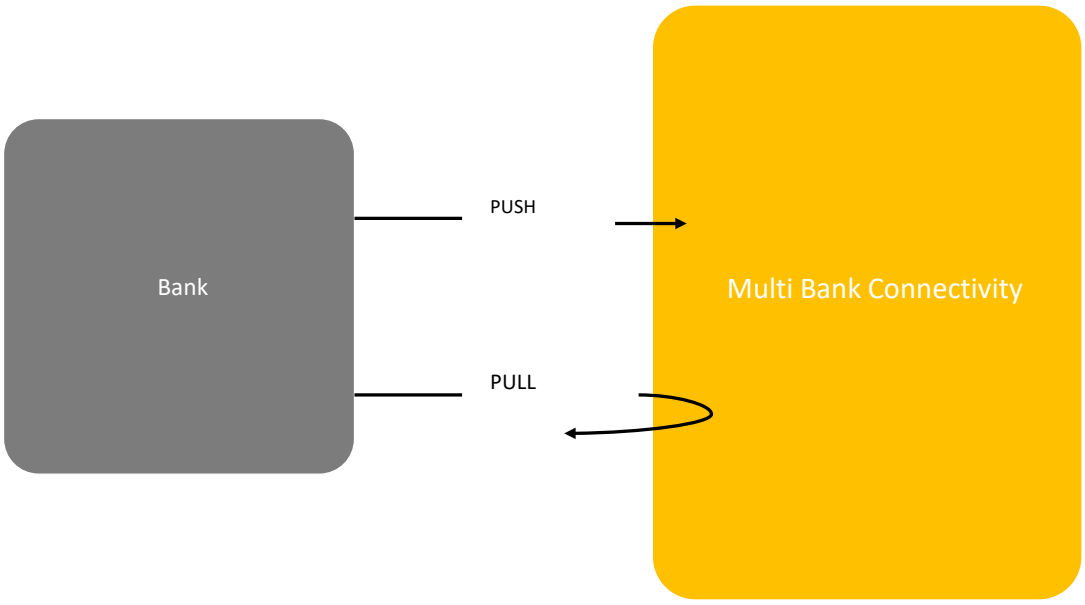
An SFTP server is hosted by the Bank. SAP MBC tenant acts as SFTP client

Inbound

MBC tenant pushes file to **SFTP @Bank inbox**

Outbound

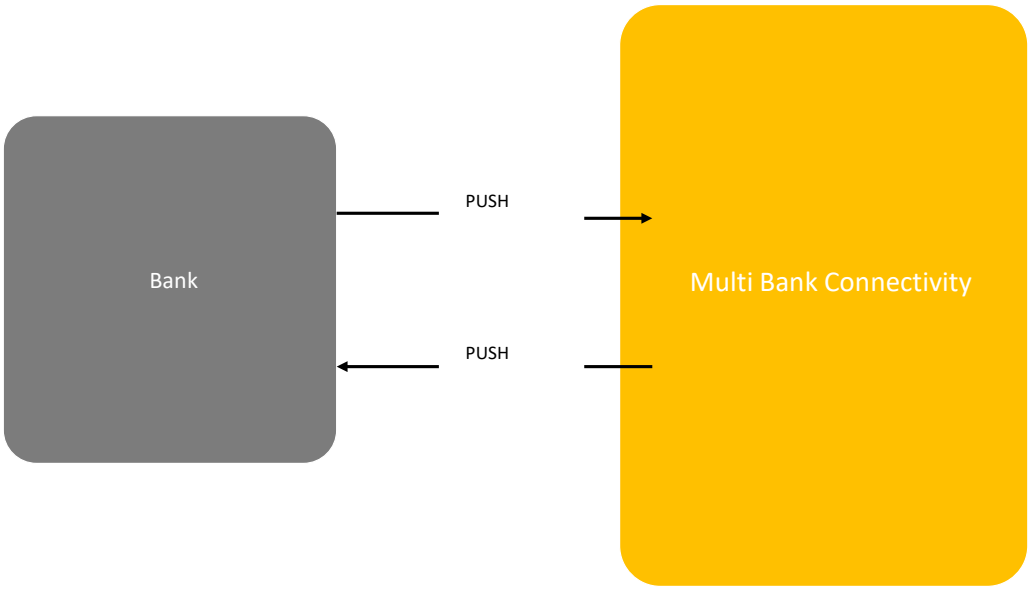
MBC tenant pulls responses from **SFTP @Bank outbox**



5.3.2 Push/Push - Default for Webservices

In this scenario, SAP MBC pushes data to the Bank's hosted server and the Bank pushes response and reconciliation data back to SAP MBC.

Note.: If these scenarios are not suitable for your organization, please inform SAP in the questionnaire.



6 Security Requirements

To set up a secure connection between a customer system and MBC, 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 whitelist SAP IP ranges depending on your firewall position.

Message Level Security is optional but highly recommended by SAP for secure transfer of data.

The artifacts required depend on connectivity options and security levels.

Please note that security artefacts will be required for your test and productive systems.

The sections which follow outline requirements.

6.1 IP Whitelisting

To onboard to SAP MBC, you may need to whitelist SAP hostnames and IP ranges for SFTP, and webservice connection.

If you are using SFTP and your firewall is in front of the SFTP server, you must whitelist. Please check with your network administrator. To ensure smooth onboarding, if whitelisting is necessary, please do so before starting the onboarding questionnaire. This is a mandatory requirement.

As part of the onboarding questionnaire, you will be asked to confirm you have whitelisted the below range:

Region	Landscape Host	IP Range
Europe (Frankfurt)	*.hana.ondemand.com	IP Range
Europe (ROT)	*.hana.ondemand.com	IP Range

6.2 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 Cloud Platform Load Balancer.

As part of the onboarding questionnaire you will be asked to provide TLS security artefacts for your test and productive environments.

Please note that the same security artefacts cannot be used for your test and production environments.

In the questionnaire, you will be asked to upload your test and production security artefacts. If you cannot provide these artefacts, you can provide the date when you agree to provide each of these artefacts to SAP. Please note that providing a date is a mandatory question to proceed with the questionnaire.

6.2.1 SFTP Connections

SSH is the default authentication method for SFTP connections using the Push/Pull scenario described in section 5.3.

6.2.2 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**
>
> Please ensure that you have or procure different certificates for your TEST/QA and PROD environments, that they are signed by a trusted SAP CA, and valid for at least two years.

Related Information

- SAP Trusted Certificate Authorities

6.3 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 strongly recommended in TEST and PROD environments. In the questionnaire, you will be asked if you will be using MLS.

If you are using MLS, please ensure that you have:

PKCS7 certificates (signed or self-signed) for your TEST and PROD environments

or

PGP public keys (OpenPGP Standard) for your TEST and PROD environment

Please ensure these are available before starting the onboarding questionnaire and that they are valid for at least two years. You will be able to upload these public certificates in the questionnaire.

If you cannot use MLS, please inform your corporate customer. You will be asked in the questionnaire if you have notified the customer regarding this.

Related Information

- SAP Trusted Certificate Authorities

7 Message Types

The terms Inbound and Outbound refer to messages into and out from your organization.

Below is a list of recommended message and file formats exchanged with a corporate customer. The message type is made up of the instrument type such as credit transfer, the definition and message format, for example, PAIN.001 in XML.

There may be other format types such as SWIFT MT message types or bespoke message types specific to a corporate to bank relationship.

Please select or enter file formats you can accept, and select or enter payment status report formats and statement file types you send.

7.1 Corporate Customer Files

In this section of the onboarding questionnaire, you indicate if you support IS0 20022 Payment Message Formats. If you do support these standards, please select the formats that your system can receive from the corporate customer.

If you do not support ISO 20022 Standards, please select the flat file option and upload a sample of this file at the end of the questionnaire.

Structure	Format	Message Name
ISO 20022	PAIN.001.001.03	Customer Credit Transfer Initiation
ISO 20022	PAIN.008.001.02	Customer Direct Debit Initiation

7.2 Responses Files

In the questionnaire, please specify if you support the below Payment Status Report Format. This file will be sent from your system in response to the Corporate Customer sending a PAIN.001.001.03 or PAIN.008.001.02 file.

Structure	Format	Message Name
ISO 20022	PAIN.002.001.03	Customer Payment Status Report

In the questionnaire, please specify which Statement File Types that your system will send to the Corporate Customer.

Structure	Format	Message Name
ISO 20022 (Recommended)	CAMT.053.001.02	Bank To Customer Statement
ISO 20022 (Recommended)	CAMT.052.001.02	Bank To Customer Account Report

Structure	Format	Message Name
Delimited Text	MT940	Previous day customer statement
Delimited Text	MT942	Current day customer Report
Delimited Text (Previous or current day) statements	BAI/BAI2	Previous Day Statement or Current Day Report

7.3 Rules and Constraints of Message Usage

In this section of the questionnaire, please describe any constraints or rules that are in place regarding message usage.

Sometimes a message field may have an associated rule or constraint that is not part of ISO or other standardized rulesets. These rules may be part of an approach agreed between a customer and a specific bank.

7.4 Implementation Guideline for Message Types

In this section please indicate if you follow specific implementation guidelines for messages.

Implementation guideline documents are sometimes provided by a bank to define how the bank expects to receive a message.

Some banks may comply fully with ISO rules. Therefore, there will be no difference between their implementation guideline and ISO rules. However, in some cases, an implementation guideline contains variances that a Corporate customer needs to review as part of onboarding.

7.5 File Naming Convention

Banks require certain elements in a file name so that their systems know where to send a payment for processing.

MBC also uses a file naming convention. MBC requires certain elements in the file name to know where to route a file (receiver), how to handle the file, and how to populate the MBC Header fields based on file type. The MBC header is applied to outgoing messages from a corporate customer to a bank. The header wraps the message payload with fields such as Sender ID, Receiver ID, and Message type, used to determine routing in MBC.

In the questionnaire, you indicate if you can use the MBC file naming convention for inbound and outbound messages.

If you cannot use the MBC file naming convention, then SAP must use content in the file to route the file to the receiver.

7.5.1 Inbound from MBC to Bank

The format of the MBC file naming convention for messages from MBC to a bank is as follows:

- Corporate Customer ID - usually agreed on with the Bank, how the Bank identifies their Corporate Customer
- File Type – for example, PAIN.001.001.03; PAIN.008.001.02
- Unique Message IdD – for example, MBC Header <MessageId> element

Example: Customer123_PAIN001v3_1234567890.xml

7.5.2 Outbound from Bank to MBC

The format of the MBC file naming convention for messages from a bank to MBC is as follows:

- **Corporate Customer ID -** usually agreed with the Bank, how the Bank identifies their Corporate Customer
- **File Type** – for example, PAIN.002.001.03; CAMT.053.001.02; MT940
- **Unique Message ID**

Example: Customer123_CAMT053v2_9012345678.xml

In the questionnaire, please indicate for which files you can follow the MBC file naming convention.

If you cannot use the MBC file naming convention, please indicate what data in a message is used to determine the receiver and file type. SAP needs information about the receiver of a message and the type of message.

7.6 Sample Message Payload

Please prepare one sample payload message file (XML or flat file) for each of the following:

- Payment File (expected inbound format)
- Customer Payment Status Reports
- Customer Statements

The onboarding questionnaire includes one section to upload all sample files.

To ensure that files reach a receiver bank in the expected format, this a **mandatory** step in the onboarding process for validation purposes.

If you cannot provide sample files, please provide a date when the files will be available.

7.7 Message Implementation Guides

Please ensure that you have provided any message implementation guidelines to the corporate customer prior to completing the questionnaire.

Please also provide any message implementation guidelines in the questionnaire.

Related Information

ISO Standards

8 Sharing Questionnaire Responses

The corporate customer may ask SAP to share your answers to the onboarding questionnaire. If you are in agreement, please give your consent in the relevant section of the questionnaire.

9 Glossary

Term	Definition
Authentication	The process of confirming someone or something's identity. In the SCPI integration scenario, mutual authentication is carried out between the backend system and the SAP SCPI load balancer, and, secondly, authentication after this point against the participant. Both are realized using certificate-based authentication (X.509).
Certificate Authority (CA)	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 the SCPI integration scenario, any certificate must be signed by an SAP-Trusted CA. See section 6.
Client Certificate	Digital certificate used by client systems to make authenticated requests to a remote server. In the SCPI integration scenario, a client certificate is required by the participant, with SCPI client certificates (those of the load balancer) traded and consumed by the participant.
Integration flow (I-FLOW)	Specifies the flow of messages between two or more participants through the SCPI. An integration flow allows you to specify the following: • Senders of the message • Endpoints – define applied transport protocols • Applied measures related to message content signing and encryption • Applied mappings
Keystore	Self-contained collection of certificates and keys that are actively used in the establishment of connectivity to the SCPI
Onboarding	Process of connecting a participant to SCPI. Onboarding covers all tasks necessary to configure the connection and data exchange between a participant system and the SCPI.
Participant	Company or organization that onboards to the SCPI
Public Key Cryptography Standards (Version 7) (PKCS#7)	A data encryption and decryption standard that provides cryptographic privacy and authentication for data communication. In the SCPI integration scenario, one of the encryption standards offered is PKCS#7, which used extensively by SAP R/3 and PI.
SCPI	SAP Cloud Platform Integration (Cloud Integration) is hosted in the SAP Cloud. It facilitates the integration of business processes that span different departments, organizations, or companies.
Secure Socket Layer (SSL)	The standard security technology for establishing an encrypted link between client and server.

Term	Definition
	In the SCPI integration scenario, SSL is used in any web services connection.
Service activation	Process when a participant starts collaboration with another participant. On request, SAP activates the connection between the two participants and informs them when the connection is complete. This allows the newly connected participants to carry out message flow testing across the service prior to moving into the production landscape. A participant service activation is carried out in both a test and a production landscape.
Simple Object Access Protocol (SOAP)	XML based protocol for accessing Web Services
Transport Layer Security (TLS)	Summarizes settings that can be applied to secure the transfer on the communication path between two communication partners.
Web Services (WS)	Service offered by an electronic device to another electronic device, communicating with each other over the World Wide Web. In the SCPI integration scenario, Web Services are the preferred integration method.

10 Next Steps

1. Please perform all tasks in this guide to prepare for completing the questionnaire.

   The questionnaire captures your technical and business integration scoping choices and collects your keys, certificates and other integration artefacts where applicable.

   It is **vital** that preparatory steps identified in this document are completed before starting the questionnaire.
2. When you complete the questionnaire, the SAP MBC Onboarding Team reviews your responses and communicates the onboarding sequencing.
3. For queries relating to this guide or the onboarding questionnaire, contact the SAP MBC Onboarding Team: sapmbconboarding@sap.com

11 Important Disclaimers and Legal Information

Coding Samples

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

Accessibility

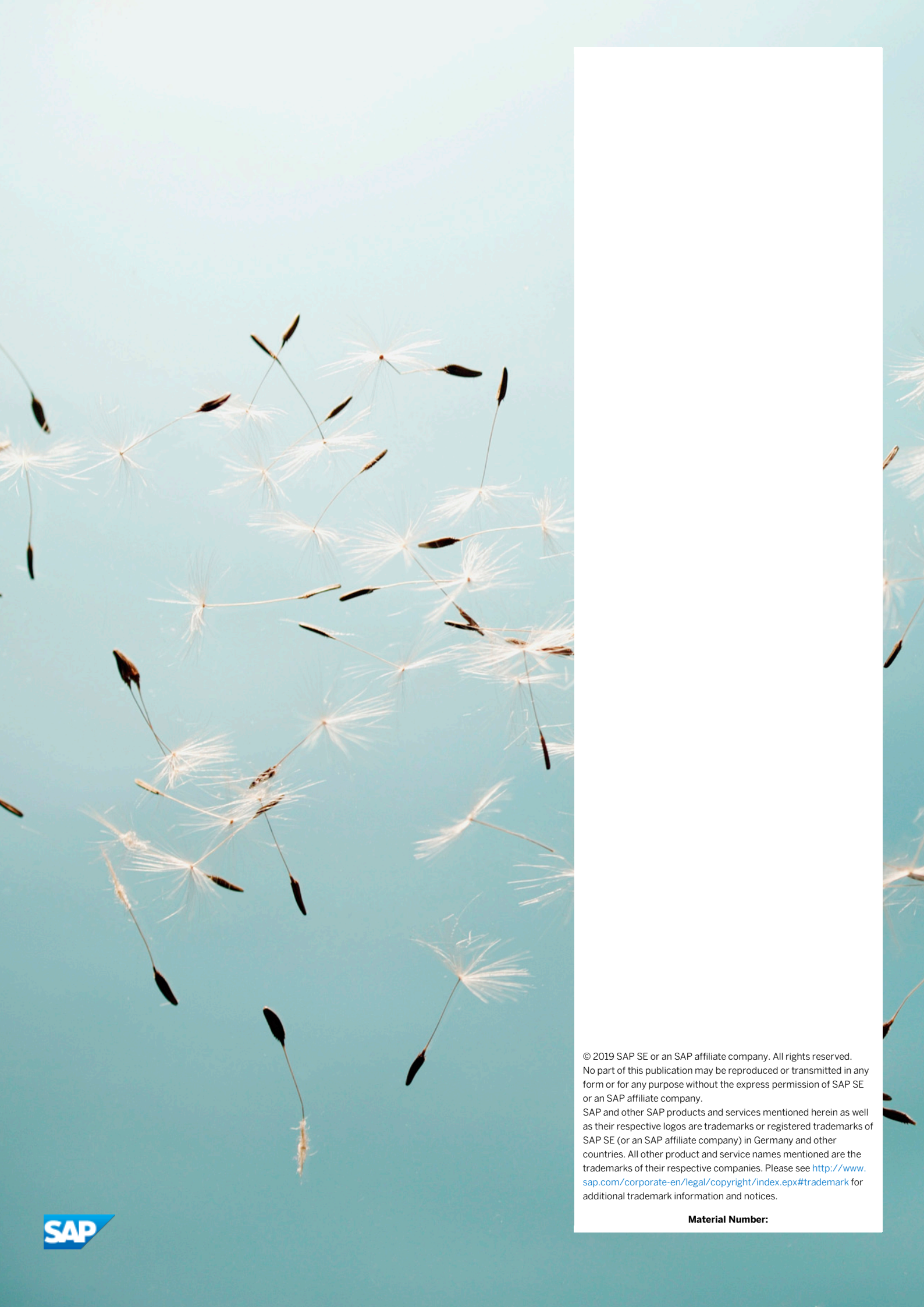
The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of wilful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

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

Internet Hyperlinks

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



Material Number: