

1. GENERAL

At the moment, your EDI application (e.g., your EDI converter) uses our interactive interface, Local User Agent (LUA) or the CDIF protocol embedded in it (for a proprietary Remote User Agent such as the PC Box client software), in order to send messages to your X.400 partners or to receive messages from them. This access technology was already on offer for the first X.400 platform at the beginning of the 1990s, but is still being provided on the current platform on compatibility grounds. This interface does not support all modern X.400 service features (e.g., FTAM Body Part, Strong Authentication), but it is good enough to transfer EDIFACT documents as text attachments or as binary attachments (Body Part 14) within a message, and this is in any case standard in the X.400 environment (TEDIS P2). For the messages, reports can also be requested and received, thus enabling a transaction to be checked.

However, it is a problem that these interfaces are not IP-based. Connections are usually made via ISDN data transfer. In individual cases, even analog modem connections are still being used. Due to Deutsche Telekom AG's IP transformation program, these transfer technologies will only be available now for a limited period, and so we would like to advise you as early as possible on alternative access technologies with the MailBox X.400 service, so that you can then consult the supplier of your application to order a new communications module or to upgrade your EDI solution, if necessary. If you purchased your solution from us (e.g., the PC Box software), we can offer you suitable successor products.

The standard protocol for access to an X.400 Message Store, and therefore also to that of MailBox X.400, is P7. All current P7 clients, such as the FileWork software which we offer (for Windows OS), or the UA-FI communications module (for Windows OS and Linux), which we also offer, are IP-enabled. The newest versions of FileWork/UA-FI also support IPv6 and with TLS 1.2 they offer a high degree of encryption for the transfer, which according to the German Federal Office for Information Security (BSI) will offer sufficient protection for the next 5 years at least. In the event of a switch to the P7 access, nothing about your X.400 address will change and you will be able to access messages delivered to your mailbox or send messages to your partners as before.

As an alternative to this standard access, with MailBox X.400 it is possible for you to transfer messages via host interfaces that are set up on different variants of the MessageGate module and use transfer protocols that are widespread on the Internet and throughout the IP world:

1. The MessageGate File Interface offers a file interface with access via SFTP or https/WebDAV.
2. The AS2 Gateway enables the connection of applications that use the EDIINT Applicability Statement 2 standard (AS2, RFC 4130) for data transfer.
3. The OFTP access enables the connection of applications that support the Odette File Transfer Protocol in version 2.0 (OFTP2, RFC 5024) or V1.4 (OFTP1).

However, with these solutions no mailbox is provided where the messages can be temporarily stored and must be retrieved, and instead there is active delivery to the transfer directory or to your AS2 or OFTP solution. However, your partners will at best recognize from the Global Domain Identifier (GDI, consisting of the country code, ADMD, and PRMD names) of your X.400 address that you are using these accesses. With the MessageGate File Interface and the OFTP access, there is even the possibility of continuing to use the existing mailbox address.

For all of these accesses, the central EDI function can be activated that simplifies the transfer of EDIFACT documents. Administration of the relevant partnerships and status reports is carried out by means of WebConfig, a web-based configuration tool.

The text below describes the various access technologies in detail and also explains the effects on your applications during migration.

2. P7 INTERFACE

As already mentioned in the General section, P7 is the standard interface for access to an X.400 mail client at a Message Store. Here the send, retrieve, list, and delete, actions can be performed on messages. All modern P7 clients support access via IP and when using the Internet also support encryption by means of TLS. Of course, this also applies to the communications modules we provide: FileWork for Windows 32 Bit/64 Bit OS (full-fledged mail client with graphic interface and MAPI/script interface for automated processing), UA-FI for Windows 32 Bit/64 Bit OS and UA-FI for Linux (simple communications modules with file interface). UA-FI for other Unix versions may be purchased from the client software manufacturer (<http://www.addonmail.com>). Many software manufacturers in the EDI environment have integrated these modules into their applications or have developed their own P7 communications modules for their converters or SAP solutions. A list of the manufacturers known to us can be obtained via our help desk.

The switch to a P7 communications module should not have any influence on the existing X.400 partnerships, because nothing about your mailboxes' X.400 address changes and these clients are normally also backwards-compatible with CDIF clients. An attractive side effect of switching to a P7 client is that the connection times are considerably reduced (cost reduction), mainly when connecting via the Internet and sending larger messages .

However, the disadvantage when integrating P7 solutions into the IP infrastructure – mainly for larger companies – is that the transfer of OSI protocols (P7, FTAM, etc.) defined in RFC 1006 is hardly taken into account with proxy solutions and firewalls. Test here the use of the Stunnel program (encrypts any TCP/IP connections by using TLS) on a separate proxy server. If this is not an option for you, please examine the use of the host interfaces described in the next sections.

3. MESSAGEGATE FILE INTERFACE

Using the MessageGate File Interface is particularly advisable if you are not using any AS2 and OFTP solution and your EDI/converter solution provides or expects data via a file interface. By using suitable transfer software for SFTP or https/WebDAV, the MessageGate transfer directory can be activated as a local drive and the usage data can be sent directly as X.400 messages. The great advantage compared with your previous solution is that you do not have to explicitly retrieve from your mailbox messages that

Ver 1.0

your partner has sent, and these or their contents can be directly delivered as files to the file interface where they can be immediately processed by your EDI system.

This is particularly easy if communication with your partners takes place exclusively by means of EDIFACT documents according to the TEDIS P2 approach (one EDIFACT document/interchange per X.400 message as a text or binary attachment to a partner). In this case it is advisable to activate the central EDI function. Here you must store on a one-time basis the EDI IDs that you and your partners use, along with their X.400 addresses in the relevant EDI partnerships, and then EDIFACT documents will be forwarded automatically by using the UNB header elements.

If you wish to send other types of document or multiple documents for each X.400 message, you need to start with a MIME header before the usage data, and this is also where additional information such as the X.400 address, message number, and subject are transferred. The structure of the X.400 message (format, attachments, etc.) and requesting and sending of X.400 reports can be defined for each partner in a partnership, or the standard values stored for the MessageGate account are used. Details on the possible settings can be found in the information sheet on the MessageGate File Interface and the MessageGate Manual.

Normally the X.400 address of a MessageGate File Interface account is set up with the GDI "c=de; a=viat;p=mgate", since all the messages to addresses that contain this GDI are generally delivered to the File Interface. However, as described in the General section, it is possible to use the X.400 address set up for the mailbox without changing the GDI (thus without P=mgate) for the MessageGate account as well. To do so, special routing entries need to be made in the system that only permit the delivery of messages and reports to either the mailbox or the File Interface. Thus on a particular cut-off date, the entire traffic needs to be switched if you decide to take over the address. However, in most cases it will make sense to gradually switch the partners to the MessageGate account with P=mgate and thus to continually reduce traffic via the mailbox until it can be terminated.

4. AS2 GATEWAY

Switching to the AS2 Gateway is particularly advisable if you are already using an AS2 communication module in your company. The great advantage compared to your previous solution is that you do not have to explicitly retrieve from your mailbox messages that your partner has sent, and these or their contents can be actively delivered as files to your AS2 solution.

Your AS2 account is put into "Agent" mode by default and behaves in a similar way to a mailbox. This means that a requested delivery notification (DN) is generated as soon as the data for forwarding to your AS2 solution has been transferred to the internal AS2 module. A response generated by your AS2 solution (MDN) will be implemented as a read notification (RN) if requested by your partner. Within the pre-configured lifespan of transactions (the default is 10 days), the AS2 Gateway attempts to deliver the data to your AS2 solution. If necessary, you can move the data to the overflow and retrieve it there by using WebConfig, in order to transfer it to manual processing, or to send it again.

If communication with your partner takes place exclusively by means of EDIFACT documents according to the TEDIS P2 approach (one EDIFACT document (interchange) per X.400 message as a text or binary attachment to a partner), it is advisable to activate the central EDI function and assign an AS2 ID to it. Here you must store on a one-time basis the EDI IDs that you and your partners use, along with their X.400

addresses in the relevant EDI partnerships. Then EDIFACT documents will be forwarded automatically by using the UNB header elements and you can address as many X.400 partners as you wish by using an AS2 ID (this saves on AS2 license costs). AS2 partnerships are only necessary if you wish to transfer other document types or multiple documents per message (multipart/mixed). If so, you must assign a separate AS2 ID to each partner. You can specify within the partnership when the AS2 gateway is to generate an asynchronous MDN for a delivered AS2 message. It is advisable to request this on the basis of a delivery notification (DN). Details on the possible settings can be found in the information sheet on the AS2 Gateway and in the MessageGate Manual.

With the AS2 Gateway, the X.400 address of an AS2 account is set up with the GDI "c=de; a=viat-as2", since all messages to this GDI are generally delivered to the AS2 Gateway. Unlike the MessageGate File Interface and the OFTP access, it is not possible to take over the mailbox address. Therefore you must gradually switch communication with your partners to the AS2 account with a=viat-as2 and thus continually reduce traffic via the mailbox until it can be terminated.

5. OFTP ACCESS

Switching to the OFTP access is particularly advisable if you are already using an OFTP communication module in your company. The great advantage compared to your previous solution is that you do not have to explicitly retrieve from your mailbox messages that your partner has sent, and these or their contents can be actively delivered as files to your OFTP solution. Please note here that V2.0 of OFTP (OFTP2) and TLS encryption is mandatory for Internet connections, whereas for a connection via dedicated networks, such as MPLS VPN, V1.4 (OFTP1) can also be used. However, we generally recommend the use of V2.0, since this is the only way to have all the service features of the access available.

The OFTP access can be operated in two modes, "Agent" and "Transfer" mode. This setting determines when the access produces which reports for messages that your partners send to you and how long the access attempts to deliver the data.

In "Agent" mode, the access behaves like a mailbox. A requested delivery notification (DN) is generated as soon as the data for forwarding to your OFTP station has been transferred to the internal OFTP module. A response generated by your station (EERP or NERP) will be implemented as a read notification (RN or NRN) if requested by your partner. Within the pre-configured lifespan of transactions (the default is 10 days), the OFTP access attempts to deliver the data to your OFTP station. If necessary, you can move the data to the overflow and retrieve it there by using WebConfig, in order to transfer it to manual processing, or to send it again.

In "Transfer" mode, the access behaves like a gateway. A requested delivery notification (DN) is generated on the basis of the EERP sent by your OFTP station (or an NDN on the basis of an NERP). However, the access only attempts to send the data to your OFTP station as long as this is defined by the priority of the X.400 message or an explicitly stated expiry date, and so normally for 24 hours. Then the transaction is marked as incorrect and an NDN is generated. You can still access the usage data in the overflow, but resending is not possible. Here too it is possible to move the data to the overflow, but the data can only be resent as long as the expiry date specified in the X.400 message (set by priority or parameters) has not been reached.

Which of the two modes makes better sense for your application depends on the degree of automation of your application and the way in which you wish to influence the data.

If communication with your partner takes place exclusively by means of EDIFACT documents according to the TEDIS P2 approach (one EDIFACT document (interchange) per X.400 message as a text or binary attachment to a partner), it is advisable to activate the central EDI function. Here you must store on a one-time basis the EDI IDs that you and your partners use, along with their X.400 addresses in the relevant EDI partnerships. Afterwards, EDIFACT documents are forwarded automatically by using the UNB header elements. OFTP partnerships are only necessary if you also wish to transfer other documents. Here the destination is identified either via an individual station address (ODETTE- ID of the service, where the last 6 digits are replaced by the partner's user ID) or by the user ID stated in the VDSN (virtual file name). If you have set up OFTP partnerships, you can specify there how additional information such as message numbers and subjects are to be transferred, along with the actual usage data of the X.400 message. You can also specify when the access is to generate the EERP for a transferred file. It is advisable to request this on the basis of a delivery notification (DN). Details on the possible settings can be found in the information sheet on the OFTP access and in the MessageGate Manual.

If you wish to use one message to transfer multiple documents as text or binary attachments, you need to declare this in a MIME header before the usage data, or with OFTP2 you need to transfer this information in the file description. The use of a MIME header for multipart messages and transfer of additional information such as subject and message number can be configured separately for each OFTP partnership.

Normally the X.400 address of an OFTP account is set up with the GDI "c=de; a=viat; p=oftp", since all messages to this GDI are generally delivered to the OFTP access. As described in the General section, it is possible with the OFTP access to use the X.400 address set up for the mailbox without changing the GDI (that is, without P=oftp) for the OFTP access as well. To do so, special routing entries need to be made in the system that only permit the delivery of messages and reports to either the mailbox or the OFTP access. Thus on a particular cut-off date, the entire traffic needs to be switched if you decide to take over the address. However, in most cases it will make sense to gradually switch the partners to the OFTP account with P=oftp and thus to continually reduce traffic via the mailbox until it can be terminated.