



MBR Gateway Service: AS2 Data Sheet (Medium Security Using TLS/SSL)

Technical information to configure your AS2 connection to the SEEBURGER Cloud

Company Details

Name:	SEEBURGER AG
Address:	Edisonstraße 1 DE-75015 Bretten

Contact Details

Name:	SEEBURGER Cloud Service Team
E-mail:	support@cloud.seeburger.de
Phone:	+49 (0) 7252 96 1443

To configure your connection to the SEEBURGER Cloud, please use this data sheet we prepared for you. The first information is for your network administrator to open your **firewall** for successful communication.

The second part contains the configuration data required to **send** data to the SEEBURGER Cloud, the third part includes the configuration data required to **receive** data.

In general, we want to use TLS/SSL to secure the HTTP connection AND we want data always to be signed and encrypted on AS2 level.

1. EDIINT AS2 – FIREWALL Configuration

To **SEND** data to the SEEBURGER Cloud, please open your firewall to allow outgoing AS2/HTTPS traffic:

FROM: IP address of your HTTP system

TO: IP ranges: **85.115.5.64** – **85.115.5.95** and
85.115.19.120 – **85.115.19.127**

Port: **9843**

To **RECEIVE** data from the SEEBURGER Cloud, please open your firewall to allow incoming AS2/HTTPS traffic:

FROM: IP ranges: **85.115.5.64** – **85.115.5.95** and
85.115.19.120 – **85.115.19.127**

TO: IP address and Port of your AS2 system

Note: Our firewall is already open to receive messages from you.

2. EDIINT AS2 – SENDING Data to the SEEBURGER Cloud

Our AS2 Identifier:

URL:

TLS/SSL certificate:

ENCRYPTION Certificate:

ENCRYPTION Algorithm:

SIGNATURE Algorithm:

Individual ID of your communication partner on the SEEBURGER MBR Gateway

https://as2-rs.seeburger.cloud:9843/cbr

as2-ms-ssl.seeburger.cloud.cer¹

as2-ms.seeburger.cloud.cer¹

We are supporting 3DES, AES/128, AES/192 and AES/256.

Note: We classified 3DES as medium secure. We recommend using AES/256 to meet the highest standards of security.

We are supporting SHA-1, RSA-256 (SHA-2), RSA-384 (SHA-2) and RSA-512 (SHA-2).

AS2 Message Disposition Notification (MDN):

<u>Note:</u> We classified SHA-1 as medium secure. We recommend using an SHA-2 algorithm to meet the highest standards of security.
Synchronous or asynchronous, MDN will be signed always.

3. EDIINT AS2 – RECEIVING Data from the SEEBURGER Cloud

Our AS2 Identifier:	Individual ID of your communication partner on the SEEBURGER MBR Gateway
Compression:	None
Content-Type:	EDIFACT Messages: application/edifact ANSI X12 Messages: application/edi-x12
Your TLS/SSL Certificate:	<u>Note:</u> An approved Certificate Authority (CA) should issue your SSL Certificate. Please add the domain host name used in the URL as Common Name (CN) in the certificate request and do not use a static IP as host name.
ENCRYPTION Algorithm:	We are supporting 3DES, AES/128, AES/192 and AES/256. <u>Note:</u> We classified 3DES as medium secure. We recommend using AES/256 to meet the highest standards of security.
SIGNATURE Certificate:	as2-ms.seeburger.cloud.cer ¹
SIGNATURE Algorithm:	We are supporting SHA-1, RSA-256 (SHA-2), RSA-384 (SHA-2) and RSA-512 (SHA-2). <u>Note:</u> We classified SHA-1 as medium secure. We recommend using an SHA-2 algorithm to meet the highest standards of security.
AS2 Message Disposition Notification (MDN):	SEEBURGER Cloud always requests asynchronous, signed MDNs . <u>Note:</u> Please be aware of your asynchronous MDN settings. The URI /cbr must only be used for EDI messages – not for MDNs. Use the URI that is sent within the AS2 request. If your AS2 software requires a static URL to return the MDN, please use https://as2-rs.seeburger.cloud:9800/mdn .

¹You can download our data sheets and certificates on the following URL: www.seeburger.com/cloud/connect-the-cloud/