

simply secure

IncaMail

Information security

Version: V01.15

Date: May 2022

Contents

1	Introduction	3
2	Basic principles	3
3	Connection types	4
3.1	Mail Gateway Integration (MGI)	4
3.2	Web Interface (WI)	5
3.3	Enterprise Application Integration (EAI)	6
4	Sending large files (Large File Transfer (LFT))	6
5	Processing	6
6	Scope of services of IncaMail according to dispatch types	7
7	Certification and obligations	8
8	Use of IncaMail in Europe	8
9	Technical and organisational measures	8
10	Handling IncaMail	10
11	Appendix	12
11.1	ISO27001 certificate.....	12

1 Introduction

With IncaMail Post CH communication Ltd provides a platform for confidential and verifiable e-mail exchange. Here technically and legally we rely on standards and make it possible – integrated in existing processes – to exchange information (e-mails) between users and systems confidentially and verifiably. In this regard we offer various identification and security levels oriented towards the business case / application.

Depending on the business case / application, different connection types are provided, Mail Gateway Integration (MGI), Enterprise Application Integration (EAI) or Web Interface.

2 Basic principles

To ensure information security with IncaMail, Post CH communication Ltd adheres to the following basic principles which give the acronym INCA:

- Integrity
- Non-repudiability
- Confidentiality
- Authentication

Integrity

The messages remain unchanged. Post CH communication Ltd ensures that data is not changed when it is transferred.

Non-repudiability:

Sending and receiving can be verified. When the messages are retrieved, this is documented with IncaMail. With the message type “Registered”, the sender receives proof as a digitally signed acknowledgement with a time stamp.

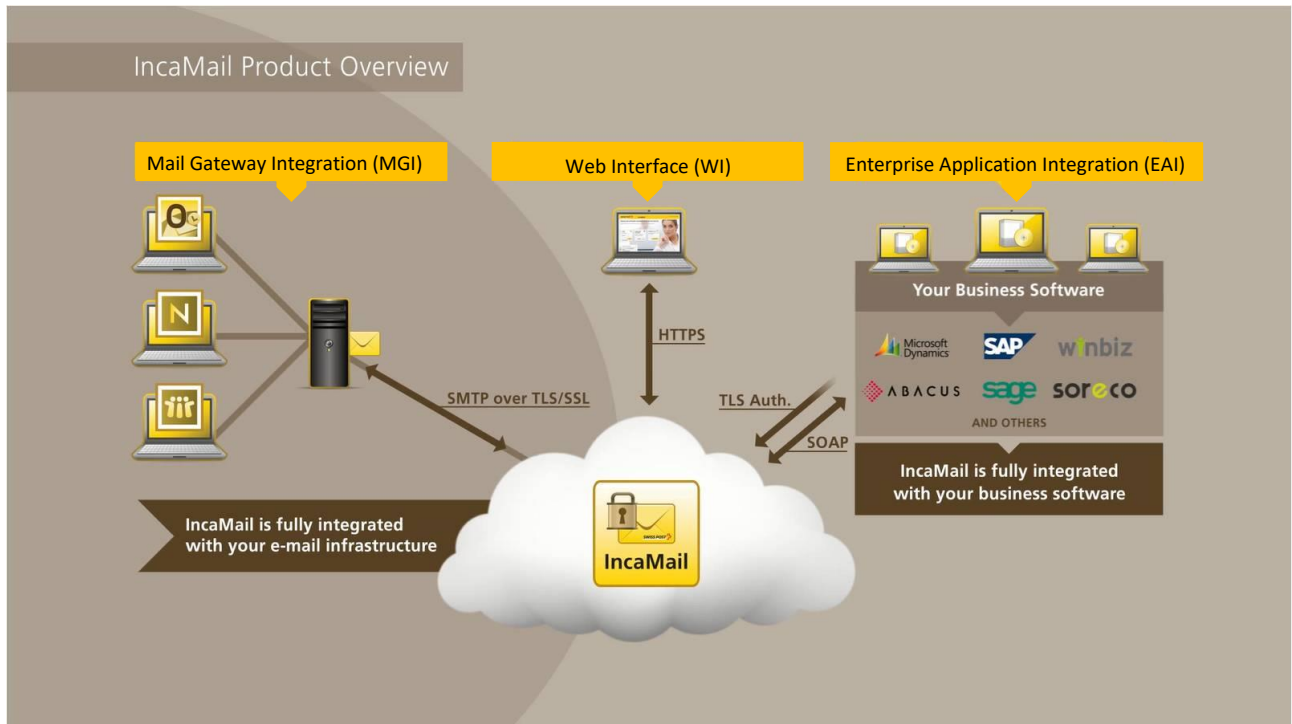
Confidentiality:

The data cannot be seen by third parties. IncaMail transfers all data via an encrypted connection.

Authentication:

The users are identified by entering their e-mail address and, if necessary, with the physical address when registering personally for the first time, and by entering the corresponding activation codes. If it is not a personal use of IncaMail but rather a company domain connection, the authentication is done via a written IncaMail service contract.

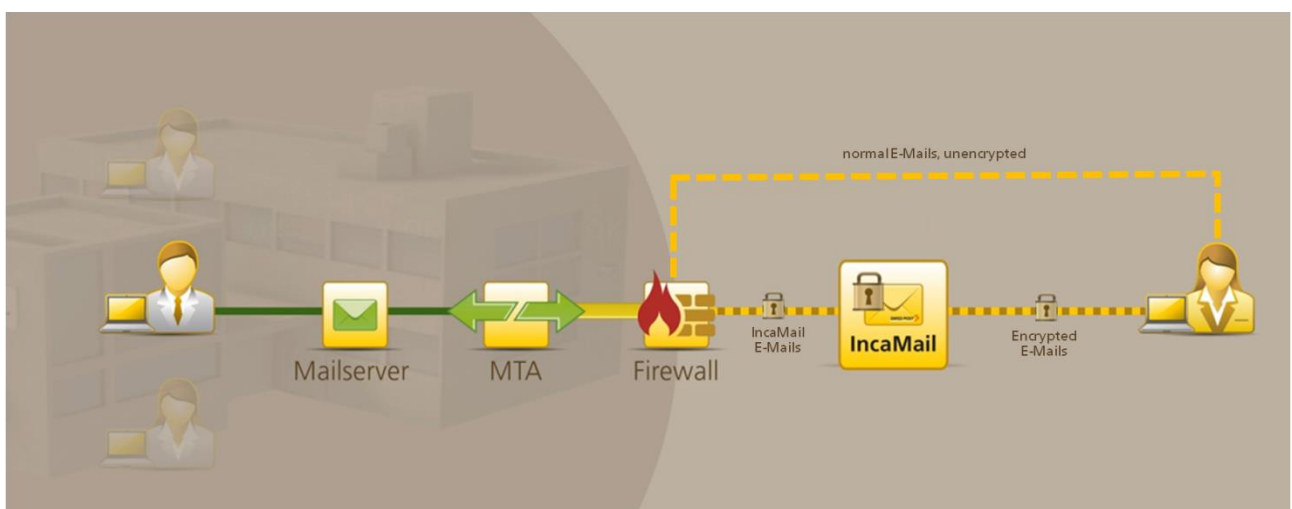
3 Connection types



IncaMail offers different connection types which are used depending on the customers' requirements. In the following chapters each connection type is explained briefly.

3.1 Mail Gateway Integration (MGI)

The customers connect their mail gateway to send and receive messages with an encrypted line with IncaMail. The gateway function is activated in the customers' own corporate network. The customers' existing mail gateway is configured by the customers so that normal e-mails are still sent and received via the customers' own infrastructure and only IncaMail messages are passed on to the IncaMail platform via an encrypted connection.

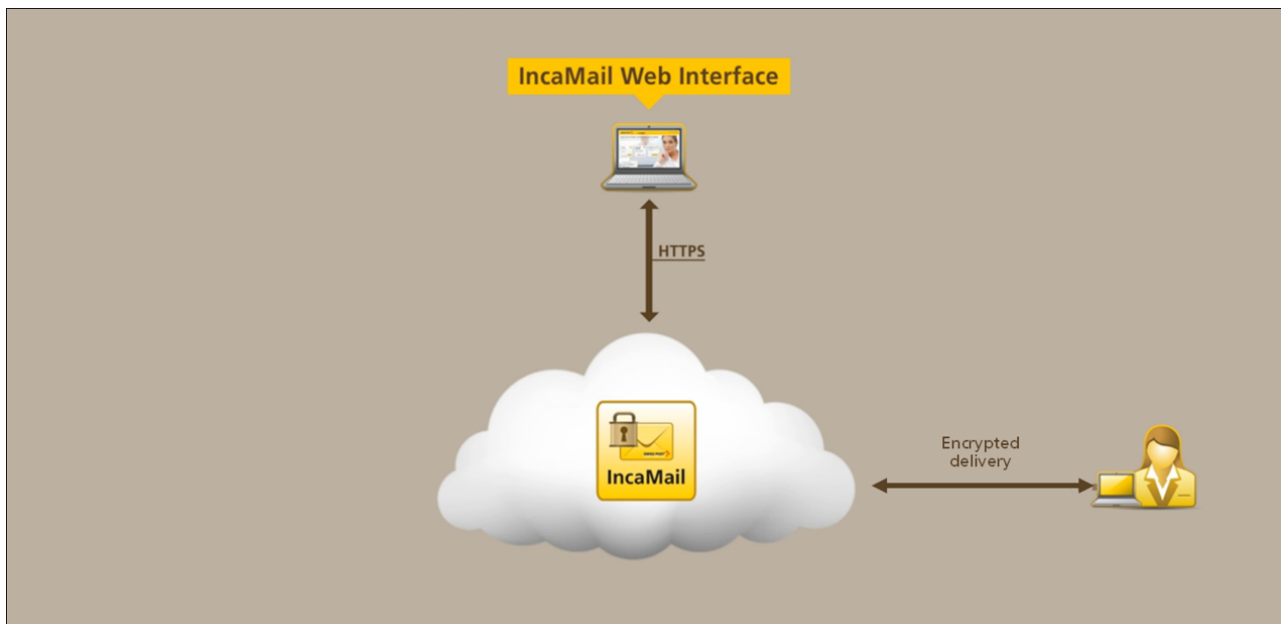


Incoming messages are sent via a secure and encrypted connection to the customers' mail gateway. With incoming messages from the customers' gateway and with outgoing messages until they are passed on to the IncaMail platform, the customers themselves are responsible for the integrity and confidentiality of the messages in their own network.

IncaMail receives only messages from the customers' mail gateway which are sent via TLS encryption (incl. certificate-authentication) and only delivers messages to the customers' mail gateway if TLS encryption (incl. certificate-authentication) can be established (enforcement). The technical connection of the IncaMail customers is therefore encrypted, with the encryption technology based on the state of the art.

3.2 Web Interface (WI)

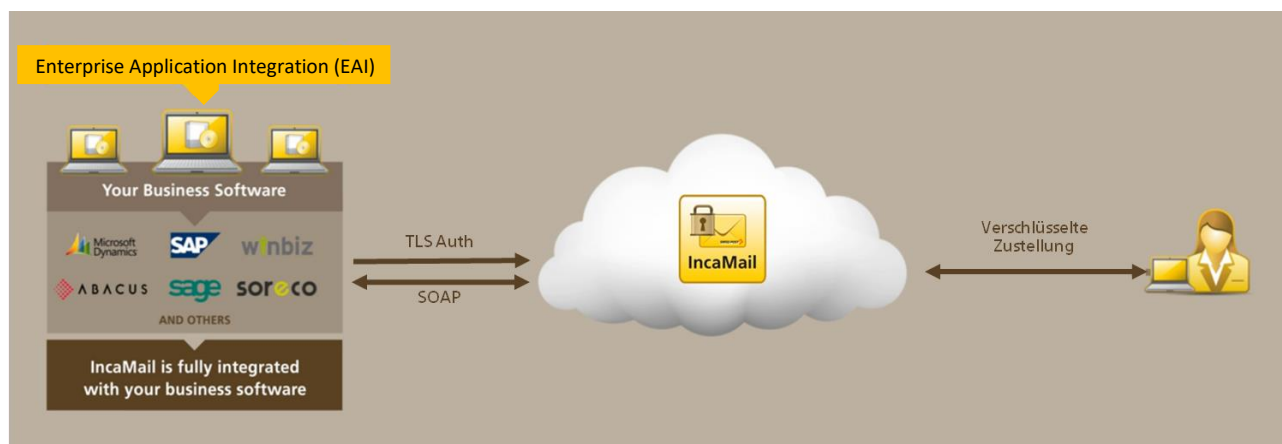
Via IncaMail Web Interface you can use IncaMail directly from your web browser and receive these encrypted e-mails directly in your usual inbox.



IncaMail can be used directly via Web Interface for sending and receiving e-mails – irrespective of your location and the end device used (PC or mobile devices).

3.3 Enterprise Application Integration (EAI)

With EAI, sending and receiving can be integrated directly in the business software.



Here IncaMail offers the two interfaces SOAP web service (HTTPS) and TLS Auth (SMTP over TLS). Authentication is via a valid user name/password.

The TLS Auth interface can be used only for sending messages.

Via SOAP web service messages can be sent and also received. When receiving messages, the encrypted messages can be decrypted via SOAP decrypt.

4 Sending large files (Large File Transfer (LFT))

IncaMail gives customers who have integrated IncaMail into their e-mail infrastructure (Mail Gateway Integration – MGI) the option of sending large volumes of data via Large File Transfer. Volumes of data of up to 1 GB can be sent securely using the [IncaMail add-in](#). No additional costs are incurred through use of the large file transfer service.

You load your files using drag and drop or by clicking on the relevant zone via a secure connection to the IncaMail server. The data is stored exclusively in encrypted form on Swiss Post's IncaMail server. Please be aware that the files are available for download from the IncaMail server for a maximum of seven days, after which they are irrevocably deleted. Once successfully uploaded, links are automatically generated in the current message, allowing the recipient to download the files. Send your e-mail to the intended recipients as usual securely via IncaMail. Since the files are not directly attached to the e-mail, they only have a minor impact on the e-mail's size.

Large File Transfer (LFT) from IncaMail can also be used as part of administrative proceedings (ECAPO, SR 172.021.2), in civil and criminal processes, and in debt enforcement and bankruptcy proceedings (VeÜ-ZSSV, SR 272.1) (see [IncaMail for public authorities](#)). IncaMail is a secure file delivery platform recognized by the Confederation.

5 Processing

IncaMail is a platform for the traceable and confidential exchange of e-mails. To support the different connection types and also the check for malware, content data is located temporarily on the platform for up to 90 days as part of the sending, retrieval and reading process. Of course this is deleted immediately after this period has ended. ISO 27001-certified processes also ensure that no unauthorised people (e.g. administrators) have access during these sending, retrieval and reading processes.

6 Scope of services of IncaMail according to dispatch types

Service	Confidential	Personal	Registered
Identification of sender	At least verification of e-mail address or business customer contract	At least verification of e-mail address or business customer contract	At least verification of e-mail address or business customer contract
Identification of recipient	At least verification of e-mail address or business customer contract	At least verification of e-mail address or business customer contract	At least verification of e-mail address or business customer contract
Authentication of sender	At least e-mail address and individual password or domain certificate (BC-MGI*)	At least e-mail address and individual password or domain certificate (BC-MGI*)	At least e-mail address and individual password or domain certificate (BC-MGI*)
Authentication of recipient	At least e-mail address, encrypted message and security code via e-mail or domain certificate (BC-MGI*)	At least e-mail address, encrypted message and individual password	At least e-mail address, encrypted message and individual password or domain certificate (BC-MGI*)
Confidentiality	Transport route encrypted BC-MGI*: unencrypted in the internal network of the business customer	Transport route encrypted BC-MGI*: unencrypted when sending in the internal network of the sending business customer	Transport route encrypted BC-MGI*: unencrypted in the internal network of the business customer
Identifiable message status	Arrived at IncaMail Delivered Undeliverable System message Read (not for BC-SI*)	Arrived at IncaMail Delivered Undeliverable System message Read	Arrived at IncaMail Accepted Delivery refused Expired Undeliverable
Logging for the purpose of traceability (journal/logbook)	Status in online logbook or business software	Status in online logbook or business software	Status in online logbook or business software Digitally signed postal receipts for dispatch and receipt
Receipt	Web interface recipients have to actively open message; BC-MGI* receive message automatically.	All recipients have to actively open message.	All recipients have to actively agree to receiving message.
Delivery	Usually within a few seconds. If there are complications: Several delivery attempts within 72 hours incl. information to sender	Usually within a few seconds. If there are complications: Several delivery attempts within 72 hours incl. information to sender	Usually within a few seconds. If there are complications: Several delivery attempts within 72 hours incl. information to sender
Legal basis	General terms and conditions or business customer contract	General terms and conditions or business customer contract	General terms and conditions or business customer contract VeÜ-ZSSV**
Other	-	-	Acceptance can be refused by recipient.

* BC-MGI = Business customers with Mail Gateway Integration. MGI is a product for integrating IncaMail directly in a business customer e-mail infrastructure.

**Ordinance from 18 June 2010 on Electronic Transmission for Civil and Criminal Trials and for Debt Collection and Bankruptcy Proceedings (VeÜ-ZSSV)

7 Certification and obligations

As already mentioned, the information security of IncaMail is based on the certified setup of an information security management system (ISMS) according to ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems – Requirements).

In Switzerland, according to the legal requirements, Post CH communication Ltd has also been recognised by the state as an officially approved delivery platform for electronic legal dealings in court proceedings and matters with authorities (eGov). Accreditation as an approved delivery platform requires fulfilment of the requirements for the architecture and technical security and also fulfilment of high operational requirements (information security and IT service management).

When dealing with customer data, Post CH communication Ltd is bound to Swiss postal and telecommunications secrecy and, in connection with IncaMail, also guarantees the level of confidentiality required in the Swiss banking world, in the insurance business or in attorneyship (banking secrecy, stockbroker secrecy, insurance secrecy, attorney-client privilege).

8 Use of IncaMail in Europe

IncaMail is used by numerous companies around the world. IncaMail's distinguishing features include the fact that the data is processed in Switzerland in compliance with Swiss and European data protection regulations and strict information and data security measures.

The European Commission has confirmed that the level of data protection in Switzerland in all forms is adequate. By adopting the protocol amending the Council of Europe's Data Protection Convention 108 and by amending the Federal Act on Data Protection, Switzerland is taking regulatory measures to ensure that data protection measures continue to remain adequate in the future.

The necessary data protection tools within the scope of the GDPR (e.g. DPA) are available to IncaMail customers.

9 Technical and organisational measures

The IT systems and other resources used for IncaMail are protected against unauthorized processing using technical and organizational measures relating to information and data security.

The IncaMail Department of Post CH communication Ltd has taken technical and organisational measures so that its internal organisation meets the particular requirements of information security to protect all sensitive data against abuse. These explanations and descriptions which refer to the IncaMail Department of Post CH communication Ltd are, in their current version, part of the documentation on information security.

Entry control

The aim of entry control is to prevent unauthorised entry to data processing systems with which sensitive (especially personal) data is processed or used.

Measures of the IncaMail Department of Post CH communication Ltd for entry control:

The IncaMail servers are in a computer centre which has a multi-level security concept and is built according to the room-within-a-room principle.

The security features include:

- The computer centre is monitored by cameras and guarded around the clock (24/7) by security staff who check the buildings both inside and outside
- All building areas are alarmed

- Without proof of identity, nobody can enter or leave the building, all visitors are compared with a customer-specific permission list
- The security systems comprise contactless keycards which are usually complemented by biometric readers and personal interlock systems

Connection control

The aim of connection control is to take suitable measures to prevent unauthorised use of data processing systems with which sensitive (especially personal) data is processed or used.

Measures of the IncaMail Department of Post CH communication Ltd for connection control:

For administrative activities the operators have to connect to a jump host via a VPN and can then access the corresponding IncaMail servers only from here. Authentication in the VPN is done via a two-sided certificate-based process. Connecting to the jump host then requires a SuisseID (advanced certificate on a hardware token). Afterwards the operator has to log on to the IncaMail server again under his/her UserID. The respective operators are given corresponding authorisation by Post CH communication Ltd.

Access control

The aim of access control is to guarantee that only those people authorised to use the data processing systems can solely access the sensitive (especially personal) data which is subject to their access authorisation and that personal data cannot be read, copied, modified or deleted without authorisation during processing, use and after storage.

Measures of the IncaMail Department of Post CH communication Ltd for access control

Access is logged in the respective systems. These logs are archived according to the company accounts decree.

Transfer control

The aim of transfer control is to guarantee that sensitive (especially personal) data cannot be read, copied, modified or deleted without authorisation while being electronically transmitted, transported or stored on data carriers, and that it can be checked and determined at which locations the transfer of personal data by data transmission facilities is scheduled.

Measures of IncaMail Department of Post CH communication Ltd for transfer control:

IncaMail is a platform for the confidential and verifiable exchange of e-mails. Here the senders and also the recipients of the e-mails are identified and authenticated.

To support the different connection types and also the check for malware, content data is located temporarily on the platform as part of the sending and reading process. Of course this is removed again immediately when these sending/reading processes are concluded. ISO 27001-certified processes also ensure that no unauthorised people (e.g. administrators) have access during these sending and reading processes. The account and transaction log data is stored on encrypted backup devices.

Input control

The aim of input control is that it can be determined subsequently whether and by whom sensitive (especially personal) data has been entered in the data processing systems, modified or deleted.

Measures of the IncaMail Department of Post CH communication Ltd for input control:

Every participant on the IncaMail platform is identified and authenticated. The corresponding activities are logged.

The activities of the operators of the IncaMail platform are logged.

Order supervision

The aim of order supervision is to guarantee that sensitive (especially personal) data processed as per order can be processed only according to the instructions of the orderer.

Measures of the IncaMail Department of Post CH communication Ltd for order supervision:

The sender selects a desired dispatch type for each IncaMail. This dispatch type determines how the IncaMails are to be processed. This processing is controlled via the SW.

Availability control

The aim of availability control is to guarantee that sensitive (especially personal) data is protected against accidental destruction or loss.

Measures of the IncaMail Department of Post CH communication Ltd for availability control:

The infrastructure is redundant and the account and transaction log data is backed up. The encrypted backups are stored in a safe at a Swiss bank.

Separation control

The aim of separation control is to guarantee that data collected for different purposes can be processed separately (limitation of use).

Measures of the IncaMail Department of Post CH communication Ltd for separation control:

IncaMail runs on dedicated servers.

10 Handling IncaMail

As a platform for the confidential and traceable exchange of information, IncaMail is integrated in an overall system (person, computer and internet) of senders and recipients, and here their security is outside the control of IncaMail.

As a user you can influence the security of this overall system, however:

- Person:
 - Make sure there is a secure password for the IncaMail Service or your e-mail service. Do not choose a password which is easy to guess. Tips on secure passwords can be found with the [registration](#) of IncaMail; when entering the password the password strength is displayed as a graphic next to the input field.
 - Your password is personal. Do not disclose it to anyone else. Use a password manager if necessary to securely store your password.
 - Make sure that the recipient address (e-mail) you enter is correct and corresponds with your desired recipient.
 - Check the right dispatch type is selected (e.g. for certain court petitions the dispatch type eGov Registered is compulsory).
 - If you are sending large attachments, use IncaMail's Large File Transfer. If this is not possible, it is recommended to clarify with the recipient in advance the maximum amount of data which can be received by e-mail. Here it needs to be taken into consideration that the message will become larger because of the encryption with IncaMail.
 - Check the acknowledgements issued by IncaMail for correctness.
- Computer:
 - Protect your computer with an antivirus program and keep your operating system and also your applications up to date (further information can be found at the [Confederation's Reporting and Analysis Centre for Information Assurance MELANI](#)).. After a transaction is completed, log off correctly from IncaMail (Link "Logging off") and empty the browser cache if you are using IncaMail via the website (www.incamail.com).

- Internet:
 - Visit only websites you trust. When logging in, check the green display of the link in the browser. Observe the [advice of the Confederation for careful surfing on the Internet](#).

A requirement for every secure online transaction or communication is that all participants carefully deal with all elements in the process. This is the case in e-banking as well as in the use of IncaMail.

11 Appendix

11.1 ISO27001 certificate



Certificate



The certification body of Swiss Safety Center AG hereby confirms that the company

Post CH Communication Ltd
Wankdorffallee 4
CH-3030 Bern



Site:
Franklinstrasse 26
CH-8050 Zürich

for the scope

Development, distribution and operation in the areas of Digital Health and E-Government

successfully applies an information security management system (ISMS) according to

ISO/IEC 27001:2013

Statement of Applicability:	21.09.2021
Registration number:	22-267-704
Initial certification:	16.11.2018
Recertification:	20.12.2021
Valid from:	01.12.2021
Valid until:	30.11.2024



Heinrich A. Bieler
Head of the certification body

Wallisellen, 06.01.2022
Swiss Safety Center AG, Certifications
Richtstrasse 15, CH-8304 Wallisellen
A company of the SVTI Group, member of VdTÜV

