Trust Service Practice Statement (TSPS) for the electronic registered delivery service E-POST

1. Introduction

1.1. Title and identifier of this document

The title and identifier of this document is “Trust Service Practice Statement for the electronic registered delivery service E-POST“.

1.1.1. References

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS regulation)

[2] BSI-Standard 100-3 – Risk analyses on the basis of the BSI Standard „IT-Grundschutz“

[3] ETSI EN 319 401 V2.2.1

[4] Termination of service scheme

1.2. Overview

Deutsche Post AG provides the communication service E-POST. Part of E-POST is a qualified trust service for the delivery of electronic registered mail according to the eIDAS regulation of the EU. For further details on all the offered services see the document “Service Description” on the product website.

This document applies only for the qualified trust service “electronic registered delivery service” according to the eIDAS regulation, which is offered under the trademark “E-POST”.

This document is a *Trust Service Practice Statement* (TSPS) in compliance with ETSI EN 319 401 [3].

1.2.1. Identification and authentication

Participants of the trust service are identified on a quality assurance level of “substantial” or higher (for details see chapter 3.2).

1.2.2. Service overview

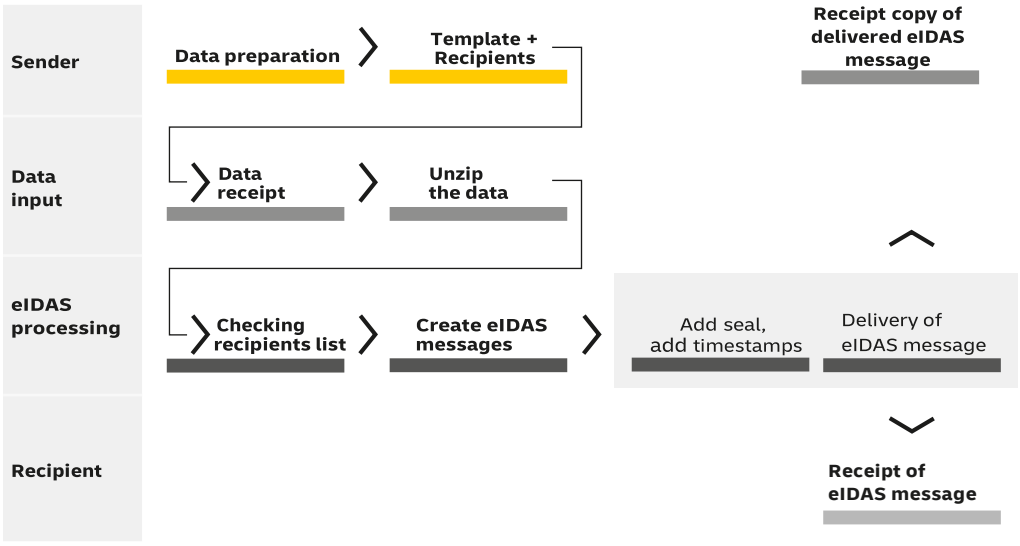
E-POST offers the delivery of registered electronic mail as a communication service between two identified customers. Part of this general service is a qualified trust service.

1.2.2.1. Sending mail

The following diagram shows the complete process of the delivery service:

- Business customers, having been validated to be qualified to send messages under the rule of the eIDAS regulation, transfer a list of recipients and the corresponding content templates of the messages in a data package to the E-POST gateway.
- E-POST receives and processes this data package.
- For every message being marked to be send as registered electronic mail, E-POST
  - confirms that the sender is qualified to send messages under the eIDAS regulation,
  - confirms that the recipient is qualified to receive messages under the eIDAS regulation,
  - generates the message in the preprocessing stage (the gateway, MKG) as part of the service agreement with the gateway customer,
  - initiates the delivery of the message,
  - cryptographically seals the message with a

Delivery Service



qualified electronic seal of Deutsche Post AG,
- adds a qualified timestamp to document the exact time the registered mail was handed over from the preprocessing unit to the E-POST delivery system,
- delivers the registered electronic mail to the recipients mail box,
- adds a qualified timestamp to document the exact time the registered mail was delivered into the mail box,
- delivers an exact copy of the registered electronic mail to the sender (receipt).

- Protected by the qualified seal and the qualified timestamps the delivered message is temper proof.
- Once the delivery process is finished successfully both sender and recipient have received an identical copy of the message.

1.2.2.2. Receive mail

In the current implementation of the registered electronic mail delivery service the recipient is always a natural person receiving the message through the E-POST web interface or the E-POST app. The recipient can check the integrity and correctness of the message within the web interface.

1.2.2.3. Reception of receipt (Sender only)

The sender receives the receipt of the send message in a folder exclusively dedicated to him on a file server, from where it can be downloaded via SFTP. The sender can check the integrity and correctness of the downloaded message following the technical instructions provided by DPAG at the beginning of the contract.

1.3. PKI participants

This subchapter lists the kind and description of the instances participating in the trust service:

Certification Authority	D-Trust (Bundesdruckerei GmbH) issues certificates for qualified seals protecting the integrity of the exchanged messages.
Issuer of qualified Timestamps	DGN GmbH issues qualified timestamps documenting the date and time of the endpoints of the mail delivery process (sending and receiving).
Identity provider	The identification and authentication of the contracting parties is done by Deutsche Post AG. The identification is relying on the established POSTIDENT services.
POSTIDENT	Identification services of Deutsche Post AG. POSTIDENT Classic, identification at a retail counter of a post shop, and POSTIDENT Video, identification through a video chat, have been successfully approved by a conformity assessment body to be used as identification means for eIDAS trust services.
Contracting parties	The contracting parties are the active customers of the trust service. This can be natural persons (private customers) or legal entities (business customers). A contract can comprise multiple E-POST addresses.
Trusting parties	The trusting parties include the still active and all former contracting parties.

1.4. Administration of the guideline

Deutsche Post AG has appointed a management body responsible for this guideline. This document is approved by the appointed manager accountable for the qualified trust service in writing or a signed email. This is documented as “released by the trust service leader” in the change history of the document.

This guideline is updated at least once a year as part of the regularly required external audit specified in the eIDAS regulation. The appointed management body stays responsible for the regular audit of the guideline and takes care, that all changes to the product or the processes are assessed for any necessity to be reflected in the guideline. Updates are always published on the website of the trust service.

The assigned product manager is responsible for updating this document.

1.4.1. Information security guideline

The implementation of the information security guideline of E-POST is part of the certification of E-POST according to *ISO 27001 / IT-Grundschutz*. Deutsche Post AG is fully responsible for the observance of the information security guideline, even if parts of the functionality of the service are outsourced to external partners.

All external partners are obliged to observe the security policy ISTM of Deutsche Post DHL Group. The conformity is assessed by Deutsche Post using internal audits or by means of independent *ISO 27001* certification of partners.

The information security guideline and the IT setup are approved by E-POST management as part of the *ISO 27001 / “IT-Grundschutz”* certification of E-POST.

1.5. Glossary and abbreviations

eIDAS regulation	See [1] in the chapter “1.1.1 References”.
Customer	See “Contracting parties” in the chapter “1.3 PKI participants”.
Communication partner	Communication is achieved in between two (or more) communication partners through the exchange of messages. Every communication partner is identified by his or her E-POST address. A contracting party of E-POST may use multiple E-POST addresses.
Trusted message	An electronic letter delivered between two communication partners, fulfilling all requirements of registered electronic mail according to the eIDAS regulation.
Trusting party	A natural person or legal entity relying on the trustworthiness of the trust service.
Trust service	See the glossary in the eIDAS regulation.
Trusted communication	The delivery of a trusted message within a trust service.
E-POST	Trademark of the trust service addressed by this statement.
TKG	Telekommunikationsgesetz (telecommunication law). Federal German law ruling all telecommunication services.

2. Responsibility for the publication and repository

This guideline is published and made available on the website of E-POST.

All changes to this document are notified beforehand to the appointed supervisory body "Bundesnetzagentur" (BNetzA).

3. Identification and authentication

All contracting parties of the trust service are identified according to the requirements of the eIDAS regulation. All used identification processes and systems are approved by a qualified conformity assessment body.

3.1. Account identifier

Within the service all communication parties are identified by their E-POST address. Every address is following the format "<'first name'.'family name'[.number]>@epost.de for natural persons or "'employee name'@<'company name'>.epost.de" for legal entites, whereby the system takes care the part enclosed in the brackets "<>" is a unique identifier. Example: "max.mustermann@epost.de" could be the E-POST address of Max Mustermann as a natural person (private customer), whereas "max.mustermann@deutschepost.epost.de" would be his account he uses to communicate as an employee of Deutsche Post AG.

3.2. Proof of identity

All contracting parties are identified an a quality assurance level of "substantial" or higher. The identification processes are approved by a conformity assessment body.

3.3. Termination of contract

All contracting parties have the right to terminate their contract in accordance with the underlying general terms and conditions. After termination of contract the account can no longer be used for communication services. Still stored messages can be exported to the local computing device of the user. After a grace period the account is finally blocked and any remaining messages are deleted.

4. Security Controls on management, functional and physical level

4.1. Physical security controls

As physical access to the computer systems of the trust service exists, this access has to be protected properly to guarantee the trustworthiness of the service. This is confirmed as part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST. All servers are mounted in locked racks within an ISO 27001 / "IT-Grundschutz" certified data center. Physical access is restricted by multiple barriers and monitored by an electronic access control system.

4.2. Functional security controls

Functions and responsibilities are segregated whenever possible to prevent tempering or accidental alterations of the systems the trust service is based on. In areas where it's not possible to enforce a strict separation of concerns additional preemptive and counter measures are implemented.

Important security measures are the appointment of an independent information security officer, an independent data protection officer, strictly defined processes for administrative access to and audit trails of all critical interactions with the systems.

Audits of the correct implementation of the separation of concerns and all protective measures are part of the *ISO 27001 / "IT-Grundschutz"* as well as the "*Trusted Site Privacy*" certification of E-POST.

4.2.1. Separation of concerns

Deutsche Post AG implements the following trusted rolls to ensure a trustworthy operation of the electronic mail delivery service:

- **Information security officer (ISO):** Responsible for the implementation of all security measures and the regular conformity assessments and audits. The ISO is appointed by the management according to the security guideline ISTM of Deutschepost DHL Group.
- **System administrator:** Responsible for the availability of the service. He is enabled to run installations and updates on the system. In addition he is responsible for backup and restore. The system administrator is appointed by the operations manager and (in procuration) by the ISO.
- **Teleworker (DevOps):** Responsible for the development and upkeep of allocated parts of the services. All "teleworkers" are confirmed in their responsibility by the operations manager and (in procuration) by the ISO.
- **Data protection officer:** Responsible for the coordination of all data protection aspects of the service. Is appointed by the DPDHL Group data protection management.
- **System auditor:** The system auditor is entitled to review the archives, audit trails and audit protocols of all systems underlying the trust service. This role is included in the ISO role.
- **Accountable manager:** The manager accountable for the trust service, the director of the trust service, is officially nominated by a member of the board of the "Post – eCommerce – Parcel" (PeP) Division of Deutsche Post DHL or in procuration by an authorized senior manager.

4.2.2. Incident management

E-POST has implemented an incident management according to *ISO 27001 / "IT-Grundschutz"*.

The systems are under constant surveillance by security experts evaluating potential security events. In addition log files of the applications and network protocols created and analyzed. Discovered attacks will be blocked at the boundaries of the trust service.

Data protection issues are especially taken care of to prevent unauthorized access or recording of personal data.

An ISIRT team is available to immediately take care of incidents. A manager on duty is on call 24/7. A process is established to inform all supervisory bodies about any relevant security incident or loss of integrity. Deutsche Post DHL has implemented a standard process to inform all affected customers (natural persons or legal entities).

Critical security breaches will be mitigated within 48 hours.

4.2.2.1. Notification requirement

E-POST notify, without undue delay but in any event within 24 hours after having become aware of it, the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of

any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

4.2.2.2. Risk assessment

E-POST has implemented a risk management system according to the BSI standard [2].

4.2.3. Auditing process and responsibility

Processes and risks concerning the eIDAS trust service are monitored on a regular bases. The monitoring is controlled as part of external audits.

These external audits are conducted annually as part of the *ISO 27001 / "IT-Grundschutz"* audit and every second year as part of the conformity assessment of the qualified trust service.

4.3. Security controls of the workforce

Deutsche Post AG ascertains, that all employees, contractors and partners involved in providing the trust service, maintain their trustworthiness. This is part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.

Deutsche Post AG has implemented a process to ascertain that all personnel possess the required know-how, expertise, qualification and responsibility for their assigned tasks. Deutsche Post AG secures that the workforce handling personal data are regularly (at least once a year) trained in data protection and IT security measures. Access to sensitive data and/or systems is restricted to personnel being formally approved by the management and IT security organization. Violations of IT security regulations and/or this guideline are handled according to the standards of the security policy of Deutsche Post DHL Group.

As outlined in the ISTM, the management of Deutsche Post AG has nominated an Information Security Officer (ISO). The Information Security Officer has officially consented his nomination.

All employees of Deutsche Post AG and all contractors working for the trust service are bound to the regulations of the ISTM. Roles are taken by different personnel to circumvent conflict of interests. All areas, where this principle cannot be adopted, are kept under strict controls.

All essential roles of the qualified trust service are staffed in a formal process by the accountable senior management body.

Access to sensitive data is restricted by technical measures and limited to the unavoidable minimum.

The management body has implemented processes and appointed experts to ensure, that decisions concerning the trust service are made taking into account the necessary experience, know-how in security measures and the operation of IT systems.

4.4. Audit trail

E-POST uses a centralized logging for all application and system protocols. Administrative tasks are logged revision proof in a separate system. Any messages processed by the system are only logged as required by telecommunication law (TKG).

4.5. Archiving

Proof of identification of contracting parties are stored in an external system for at least 5 years. Electronic mail messages are exempt from archiving.

4.6. Backup and recovery

Backup and recovery procedures are documented, recovery tests established and regularly exercised.

The data center is backed up by an independent, locally separated facility to avoid a single point of failure. The backup and recovery of the timestamping and sealing service is provided by "secunet Security Networks AG".

In case of cryptographic incidents like impaired keys of seals or timestamps or broken algorithms, the following procedures will be followed:

- reception of further messages is immediately stopped,
- if private keys are compromised, the supervisory body will be informed,
- impaired seals are deactivated,
- replaced seals are activated,
- in case of integrity breaches or suspected manipulations of messages the affected customers are informed.

4.7. Termination of the service

The process and handling of the termination of the service is described in detail in the separate document [4].

Before termination Deutsche Post AG will execute the following steps:

1) All contracting parties and otherwise involved parties of the trust service will be informed. Otherwise involved parties will be informed only through a termination notice on the website of Deutsche Post AG or through a press notice.
2) All contracting parties will be given notice.
3) Secret cryptographic keys will be destroyed or revoked (certificates).
4) The supervisory body will be informed.
5) In case of insolvency of the trust service provider all rights and obligations are inherited by the legal successor. If no legal successor can be found, the proof of identification data of all contracting parties is handed over to the supervisory body in digital form.

5. Technical security controls

Access to the systems underlying the trust service are restricted and properly protected., to safeguard the trustworthiness of the electronic delivery service. Deutsche Post AG ascertains, that all employees, contractors and partners involved in providing the trust service, maintain its trustworthiness. This is part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.

5.1. Computer access controls

Access rights, especially for privileged roles, are limited to the absolute necessity for the tasks involved. All administrative actions are logged in revision proof audit trails, guaranty that any misuse will be made accountable.

All system and network configurations incur regular inspections. Access to system configurations of the trust service require two factor authentication (2FA). System access is further protected by an additional access control layer.

The systems of the trust service are under constant surveillance to detect hacking attacks or other types of information security incidents. Specialized staff monitor the

detection of malware or alien software. Security patches are installed following a documented approved protocol. Required "out of band" patches are approved and released by experts in the field.

5.2. Lifecycle management

All facilities necessary for the provisioning of the trust service are protected by adequate means to ensure the trustworthiness of the electronic delivery service. Deutsche Post AG ascertains, that all employees, contractors and partners involved in providing the trust service, maintain their trustworthiness. This is part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.

Development of the software abides security best practices and includes security audits and penetration tests. New software is released following documented and revision proof clearance procedures.

Data storage devices are not allowed to be removed from system installations partaking in the trust service without written consent of the ISO. If there is lack of proof, that all stored data encrypted, data devices are disposed according to ISO 66399 protection class 2 or higher.

All data is stored in redundant systems in separated fire zones. Hereby the data is also protected against loss due to technical defects in a storage media.

A documented process for access control ensures that access rights for new or leaving employees, as well as employees with changing responsibilities, are processed in a timely manner and therefore eliminating unnecessary access rights. Access rights are reviewed regularly.

5.3. Network security controls

The network is partitioned into separate segments for applications, administration and protocol tasks. Each partition is protected by a firewall with a default "deny all" configuration. Procedures to change and verify firewall configurations are documented and established.

All network traffic is either taking place purely inside a single protected data center or encrypted for exchange between separate data centers.

Data exchange between the systems of the trust service and other systems is cryptographically protected to ensure the identity, integrity and trustworthiness of the remote system. Equivalent measures also protect data exchange between the critical system components within the trust service.

All data centers have redundant an independent connection to the internet.

All external and internal IP addresses are under constant surveillance (penetration tests) to identify weaknesses or other security threats. All external access points are protected by firewalls.

5.4. Timestamp

The timestamping of operational data is employing a Stratum 2 -time source.

All registered electronic mail delivered by the trust service are timestamped using a qualified timestamp, provided by an external qualified trust service for timestamps. Only the hash values of messages are transferred to the external timestamping service.

5.5. Conformity assessments and further audits

Besides the regular conformity assessments done by a certified conformity assessment body according to the eIDAS regulation, E-POST is audited every year to upkeep the *ISO 27001 / "IT-Grundschutz"* certification.

5.6. Cryptographic controls

The use of cryptographic protocols is an essential part of securing the trustworthiness of the electronic delivery service. This is part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.

Qualified electronic seals are used to protect the integrity of the electronic messages delivered by the trust service. The keys of qualified certificates for the seals are stored on cryptographic smartcards. The sealing service is operated by a third party and connected via secure links. Only the hash values of messages are transferred to the sealing service.

5.7. Operational security controls

E-POST uses reliable and trustable systems and products. All software developed specifically for E-POST is evaluated through appropriate procedures for trustworthiness and reliability.

With the exception of the software development process the operational security is part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.

6. Additional regulations

6.1. Rates

Fees are charged as described in the general terms and conditions.

6.2. Non-discriminatory use

Through the implementation of best practice solutions in web design E-POST offers the contracting parties non-discriminatory access to the services. As E-POST is a document based service, relying on PDF as the standard format, their contents of messages might not be accessible to all users. Only usage of the system via keyboard might incur limitations regarding the usability.

6.3. Financial responsibility

Deutsche Post AG assures, that enough financial resources are provisioned to operate the service and fulfill all obligations regarding the service.

Procedures for mediation and reimbursement of claims of customers or other trusting parties are documented in other guidelines verified by the conformity assessment body.

All arrangements, necessary to provide the trust service, with subcontractors, outsourcing partners and third parties, are subject to contracts and the code of conduct of Deutsche Post AG.

6.4. Confidentiality of operational information

Unless declared otherwise in writing by the contracting party and Deutsche Post AG, the confidentiality of all operational information is subject to German law.

6.5. Data protection

Personal data of contracting parties are protected by the EU General Data Protection Regulation (EU-GDPR)

and telecommunication law ("Telekommunikations-gesetz" TKG).

6.6. Liability limitation

Deutsche Post AG is responsible to perform the service subject to German law and ETSI EN319 401.

Deutsche Post AG ensures, that enough financial resources are available to recompense for any deliberate or negligent violation of the eIDAS regulation or the German trust service law ("Vertrauensdienstegesetz" VDG) by Deutsche Post AG.

Deutsche Post AG is not liable for

- any harm caused by non-disclosure of their access credentials by a contracting party,
- failure to fulfill its obligations due to faults or security issues of public institutions,
- failure to fulfill its obligations due to force majeure.

6.7. Damage compensation

Deutsche Post AG provides the trust service "electronic registered delivery" subject to the regulations and procedures declared in this policy. Deutsche Post AG makes sure all regulations named in this policy are observed. Deutsche Post AG complies with the security regulations for delivery services according to the eIDAS regulation.

The upkeep of the qualified status of the trust service is subject to audits from an accredited conformity assessment body at least every second year.

In addition Deutsche Post AG will be maintaining the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.

Operational records of the trust service can be handed over to trusting parties as evidence in legal proceedings (see chapter 6.10.4).

Deutsche Post AG assumes no further liability.

6.8. Mediation

The court having jurisdiction for the settlement of all dispute concerning the trust service is the court in Bonn, Germany.

6.9. Applicable law

This agreement is based und subject to the law of the Federal Republic of Germany.

6.10. Further regulations

6.10.1. Obligations of the users

Contracting parties are obliged to protect their access credentials. Furthermore contracting parties are committed to regularly check their inbox in the delivery service for any new messages. The contracting parties are solely responsible for creating local backup copies of sent and received messages.

6.10.2. Obligations of external organizations

To provide the trust service Deutsche Post AG is cooperating with the following organizations:

- **noris networks AG:** Hosting, administration of operating systems and internet connectivity are provided by noris networks AG. The hosting provider is contractually obliged to keep up their *ISO 27001 / "IT-Grundschutz"* certification. All procedures concerning availability, security and risk management are part of the *ISO 27001 / "IT-Grundschutz"* certification of either E-POST or the hosting provider.
- **IT Services Berlin GmbH (ITSB):** ITSB is a subsidiary of Deutsche Post AG and responsible for development, maintenance and operation of E-POST. The operation and maintenance services are part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.
- **secunet Security Networks AG (secunet):** Secunet makes a qualified timestamping service by order of DPAG provided by a third party accessible to E-POST and provides an eIDAS conform sealing service using qualified seal certificates in the form of cryptographic smartcards issued to Deutsche Post AG.
- **DGN GmbH:** Supplier of the qualified timestamping service.
- **D-Trust:** Provider of the qualified sealing certificates in form of cryptographic smartcards.
- **DPCSC:** Customer service provider for all contracting parties, as well as proofing business customer registration and identification data.

All further contractors, providing services outside of the scope of the trust service, are not listed here, but are still part of the *ISO 27001 / "IT-Grundschutz"* certification of E-POST.

6.10.3. Terms and conditions

The general terms and conditions of the E-POST service include the terms for the use of the qualified electronic registered delivery service (eIDAS delivery service). The general terms and conditions are based and subject to the law of the Federal Republic of Germany and an integral part of contract between the E-POST customer and Deutsche Post AG. Following subjects are stipulated:

a. guidelines of the trust service,
b. limitations of use of the service,
c. obligations of the users of the service,
d. information for trusting parties,
e. liability limitations,
f. constraints for loss compensations due to the use of the service beyond its constraints,
g. applicable laws,
h. mediation,
i. details on the conformity assessment and qualification status of the trust service,
j. contact details of the trust service provider,
k. commitments regarding availability of the trust service.

6.10.4. Verification management

Deutsche Post AG stores operational protocols of the trust service to be able to proof the correct operation of the service according to specification. These protocols will be provided to law enforcement officials with a valid court order or to persons under legal obligations. Event logs of the qualified trusted service provider will be stored for a maximum retention period of 30 days. Proof of identification of the contracting parties are at least stored for a retention period of five years.

No independent records of message exchange between communication partners are stored. Sender and recipient both receive an identical copy of the

exchanged message, which can be validated outside the systems of the trust service. The protocol of the trustworthy delivery of the message, the electronic registered mail delivered by the trust service, is part of the message itself. The messages are cryptographically sealed by a qualified electronic seal of Deutsche Post AG and include qualified timestamps of the exact date and time the message was send and delivered respectively. As both sender and recipient hold their own copy of the message, both can independently validate the integrity of the message by validating the seal and the timestamps.
All further records are maintained according to German telecommunication law.

2020-01-14