OSCI Transport 1.2

– Design Principles, Security Objectives and Mechanisms –

OSCI Leitstelle

Bremen, May 2002

Table of Contents

OSCI Transport 1.2

– Design Principles, Security Objectives and Mechanisms –

OSCI (Online Service Computer Interface) is a messaging standard for e-government currently being developed, in a process of extended discussions and cooperation with the German federal government, the federal states and local communities, under the leadership of the "OSCI Leitstelle" in Bremen on behalf of KoopA ADV.

OSCI was designed to allow complete and binding online e-government transactions to be carried out on the Internet by using digital signatures. This requires a high level of interoperability for both the content data and also for transport and security functions. Additional attention must also be paid to the rules and regulations that public trade is subject to. OSCI design decisions were based on these requirements.

As part of version 1.2 of the specification this document describes these requirements in detail. It starts with descriptions of general design principles and the requirements for OSCI from an e-government perspective. Scenarios for internal and external security risks are then presented. These illustrate the security objectives that were taken into account when planning the OSCI standard. Using the formal OSCI specification as a guide, the components of an OSCI message and OSCI security mechanisms are presented. A detailed discussion follows on how individual OSCI security mechanisms meet the security objectives.

No mention is made of security mechanisms apart from OSCI. A separate OSCI operational concept document will present in detail measures for improving server and building security as well as firewall systems and filter rules.

1. Design Principles

OSCI encompasses both technical/content aspects and functions for transport and security including support of digital signatures.

This document, Part A version 1.2 of the OSCI specification, also known as OSCI Transport 1.2, deals mainly with OSCI transport and security functions while OSCI technical/content requirements are summarised in Part B of the specification.

Version 1.0 of the OSCI Transport specification has been available since November, 2000. Based on this version products have been implemented and valuable experience has been gained in Bremen. This experience has lead to additional requirements which are now included in version 1.2 of this specification.

OSCI Transport 1.2 describes the data exchange format through an automated interface for the secure transfer of messages using digital signatures via the Internet or other comparable communication media.

OSCI is used for the secure transfer (according to the German Digital Signature Act) of business transaction data between two communication partners. This communication is supported by an intermediary that besides transferring the messages offers additional services via OSCI. Domiciliation for services is not handled via OSCI Transport.

The transport of OSCI messages is based on both the e-mail model and online transactions with the following design principles:

- Interoperability:
  OSCI can be used for any kind of business processes and allows the use of digital signatures (in compliance with the German Digital Signature Act) and secure transfer of digital documents between public administration and/or companies and their customers. Making the OSCI protocol an open standard ensures the development of products conforming to OSCI and guarantees continuing development and improvement of the standard.
- Scalability:
  OSCI enables the application of different security levels. An example of this could entail the use of advanced digital signatures for simple business transactions, while qualified or accredited digital signatures could be used for transactions requiring written records. OSCI nevertheless does not absolutely require the use of digital signatures.
- Application independence:
  OSCI is universal and can be used completely independently of any online application.
- Platform-independence and portability:
  OSCI uses XML technology and is operating system independent.
- Open user group:
  OSCI has no explicit user administration, but works with an open user group. Users of the application don’t have to be explicitly registered as online users first. But because internal addressing in OSCI is accomplished using encryption certificates, the possession of such a certificate is required to take full advantage of the services provided by OSCI Transport. The recipient in particular must possess an encryption certificate. A sender can to a very limited extent also send messages via OSCI without an encryption certificate.
- Independence from intermediary:
  By strictly separating content data from usage data, the intermediary receives no informa-

tion about the contents of the business transaction. The intermediary functions as a classical forwarding agent.

- Compliance with the German Digital Signature Act:
  Documents transferred via OSCI can be digitally signed in conformance with the German Digital Signature Act, i.e. the author of a document can select from an advanced, qualified or accredited digital signature when signing documents (see Appendix for the legal requirements for electronic business transactions).

Complete platform-independence has a strong influence on the security concept of OSCI. This is related to the objective of implementing security primarily on the OSCI level, as independent as possible of the security standards used in other components, e.g. the carrier network and the operating system and browser being used.

Being platform independent still does not mean that there are no requirements being made on the OSCI Transport architecture, especially for operating the OSCI platform and the user‘s backend system. Proper operation of each system is in fact a basic premise for OSCI and is presented in a separate operational concept document.

2. OSCI Communication Model

2.1 OSCI Role Model

OSCI takes into account both communication of public administration with customers (the general public and companies) by offering and handling administrative services on the Internet and also internal communication between different public administration offices and departments. Because there are so many possible scenarios in such an environment there are many functional and security-related requirements that result in a very specific communication/role model for OSCI.

The basis for all digital communication is the transfer of data from a sender to a recipient. It’s important to remember that in general several people are responsible for the content of messages by working on it together or by giving approval or consent, while only one person actually sends a message. There are different sets of responsibilities for each of these two roles. Responsibility for content lies with the authors, while the sender is responsible for sending the message to the correct recipient at the correct time. On the recipient side there is a similar difference between the recipient who receives the message and the readers of the message who work with the actual content. To differentiate these roles and related responsibilities OSCI distinguishes between “content data” (cf. 3.3) and “usage data” (cf. 3.2) in an OSCI message.

The following role model forms the basis of OSCI (cf. fig. 1):

1. Content data can be created by more than one entity. Each entity that generates content data is called “author” of an OSCI message. If required, authors can digitally sign and encrypt content data. Signing and encrypting content data is optional in OSCI.

   OSCI Transport 1.2 requires multiple signatures to enable more than one author to sign content data.

2. The persons for whom the content data are intended are called “readers” of an OSCI message. Each message can have more than one reader. If required, authors encrypt the content data in such a way that only the readers are able to decrypt it.

OSCI Transport 1.2 requires multiple encryption of the content data to enable optional encryption of content data for more than one reader.

3. Before being sent, the content data are supplemented by usage data (cf. section 3.2), including sender and recipient certificates, a time stamp, etc. Usage data can also be optionally digitally signed and encrypted. The owner of the signature certificate for the usage data is called the “Sender".

   OSCI messages have exactly one sender, consequently there are no multiple signatures for usage data in OSCI Transport 1.2.

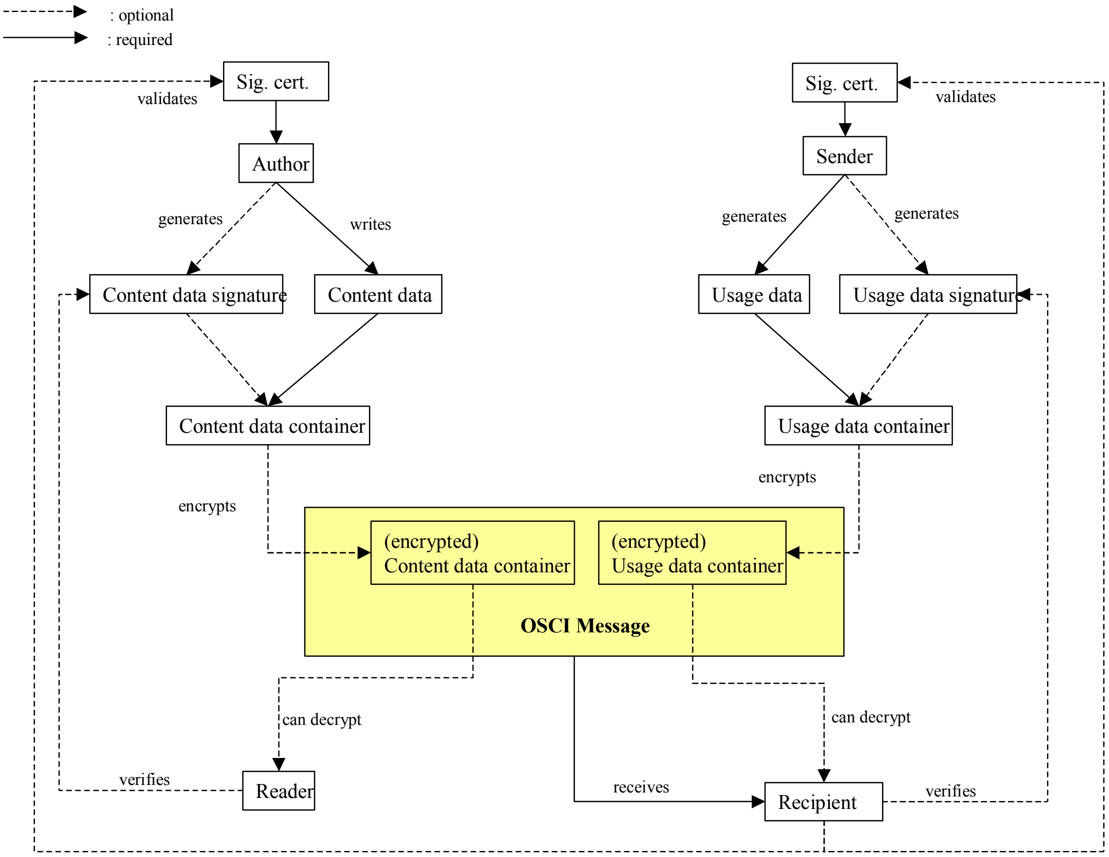


Figure 1: OSCI Role model

4. The entity an OSCI message is addressed to is called the “Recipient.” Each OSCI message is addressed to exactly one recipient.

   Consequently there is no multiple encryption for usage data in OSCI Transport 1.2.

2.2 Synchronous and Asynchronous Data Transmission

In an e-government framework there are many ways that the public can get into contact with public authorities. Higher levels of public satisfaction and efficiency are normally only attainable if a synchronous communication phase allows a dialog between client components and server components on the public administration side. By accessing existing data inventories in public administration departments the error rate for customer messages can be reduced, the quality increased and the administrative services offered made more appealing. At the end of this dialog the customer is normally presented with a form whose structured contents are sent to the administrative body. The answer to this is the subject matter of a new dialog in which the roles are reversed.

Having said this, many e-government processes are provided that are initiated by a customer message, but are not completely machine processable. Modifications must frequently be made by hand by a clerk on the public administration side. When doing so the reverse flow from administration to public must also be taken into account. In this case it cannot be a requirement for message recipients to always be available online. OSCI therefore supports not only the synchronous, but also the asynchronous exchange of OSCI messages.

2.3 The Intermediary

The existence of a central message exchange point, the “intermediary”, who can provide added value services without endangering the confidentiality of the content data, is typical for OSCI communication and is partly founded on the need for asynchronous communication. An OSCI message can be delivered to a communication partner without sender and recipient being online at the same time (cf. fig. 2).

To enable asynchronous communication the intermediary administers mailboxes for potential recipients. OSCI messages are temporarily stored in these mailboxes. Accessing the mailbox to pick up messages requires prior authentication as part of the mail fetch request . When authentication is successfully completed, a delivery request is initiated via synchronous communication between the intermediary and authorised recipients. The possession of a mailbox does not require prior registration with the pubic administration department, but is tied to the possession of an X.509v3 certificate and the mailbox is automatically created when the first message is received. Linking mailboxes to the certificate guarantees clear and unambiguous authentication for authorised recipients.

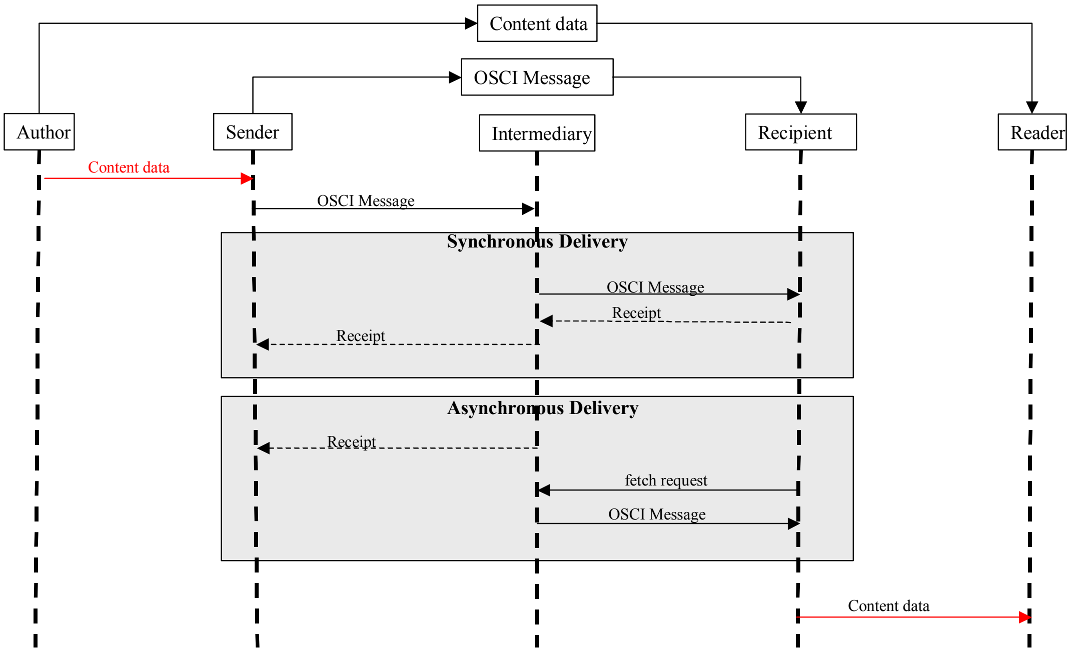


Figure 2: Synchronous and asynchronous delivery

An important aspect of OSCI communications is guaranteeing legally binding transactions and confidentiality. Business processes that are handled via the new distribution channel, the Internet, require the use of digital signatures and form an important subset of e-government. To meet these requirements OSCI is based on public key encryption technology. This is the reason why there are signature and encryption certificates for data structures on the request level. The validity of these certificates must be verified in order to make meaningful statements about their authenticity. Public key infrastructure (PKI) conforming to the German Digital Signature Act (SigG) allows the recipient to verify a signed message. However, the methods required for this are cumbersome, require intensive maintenance and are expensive. The ideal place to centralise such mechanisms is at the OSCI intermediary. Each time an intermediary inspects a certificate the results are written to a check protocol. It's up to the message recipient to use the information from the protocol to decide how to deal with the message.

It should in principle be possible for any potential recipient of OSCI messages to be able to verify certificates and signatures himself. Using OSCI infrastructure should not lead to recipients of OSCI messages relying on the intermediary's check protocol. But it is a pragmatic approach to have an intermediary provide a central location for delegating these check tasks. Because in OSCI content data and usage data are separated it is possible to do this without compromising the confidentiality of the content data as required by data protection laws. Smaller communities wishing to take a more gradual approach to introducing services on the Internet often require the economic benefits incurred by centralising these technologies.

The intermediary provides an additional service by subjecting all incoming messages to a structural check using the OSCI schema definition and offers mechanisms for establishing and securing the dialog context. Due to the tasks it carries out the intermediary takes on the roles of both recipient and sender.

The following security aspects apply to the intermediary with respect to this range of functions.

- The intermediary does not have access to the content data:
  If the content data in each business transaction are encrypted, the intermediary is still not able to decrypt and read them, even if it has a detailed knowledge of the encryption process.
- The intermediary must have full access to the usage data:
  The intermediary must be able to identify the usage data required to transfer messages.

The role of the intermediary does not always have to be assumed by a third party; this job can be handled by the department directly. In this case the department must make additional security precautions in order to do both jobs (cf. fig. 3).

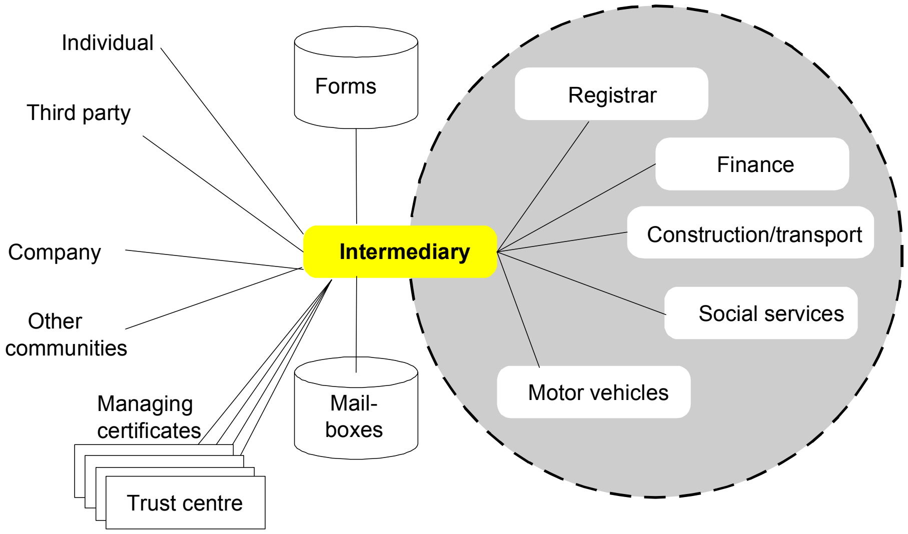


Fig. 3: The role of the intermediary

3. The Parts of an OSCI Message

In OSCI, communication between the public, intermediaries and public administration takes place on three levels using structured objects:

- The message level:
  Data on this level control the data transfer between OSCI participants communicating directly with each other. Because these data are transferred unencrypted and unsigned, they will no longer be described in this document of requirements.
- The request level:
  Usage data required for addressing are processed on this level. Usage data provide a record of data transferred and contain elements enabling a dialog to be controlled and monitored.
- The business transaction level
  Content data representing the actual business transaction are processed on this level. The intermediary has no access to these data.

To allow this separation, OSCI uses the nested envelope principle. The outer envelope contains the usage data which are required for delivery and value-added services. The content data are put into their own separate envelope which can be encrypted and signed and is placed inside of the outer envelope. It is possible to have several envelopes containing content data. If required, the outer envelope can be encrypted and signed separately from the inner envelope.

The structure of usage and content data is based on the Extensible Markup Language (XML) specification by the W3C. XML is a manufacturer-independent and open standard for the exchange of structured data and serves as the basis for processing data without media discontinuities. A valid OSCI message is a well-formed XML document. Both XML content and usage data can be encrypted and signed.

Content data are structured according to the XML schema file associated with their area of application. The definition of these schemas is independent of the structure of usage data and is handled in Part B of the OSCI specification.

In addition to the basic XML standard, OSCI uses mechanisms from the XML-based Simple Object Access Protocol (SOAP) to structure usage data, making an OSCI message a “SOAP message package”. SOAP is a powerful and easy-to-use network protocol for widely distributed architectures. SOAP is based on standard, manufacturer-independent XML technologies and creates the basis for a high level of interoperability.

Alternatively, it is possible to transfer content data in other formats via OSCI; this is done by using attachments.

3.1 SOAP Structure

SOAP is a protocol based on XML for the exchange of structured data between distributed systems. An OSCI SOAP message consists of a SOAP header, a SOAP body and any related attachments. According to the SOAP specification the message header contains the information that is updated and processed during delivery, while the SOAP body contains the static elements of the message.

The SOAP body is intended primarily for XML-formatted content data (cf. 3.3). These can be split into several “content data containers” which can be encrypted and signed independently of one another. The signature is included with each unencrypted content data container. The information required to decrypt the content data container is also included as “encryption headers” in the body. Links to them are contained in the body.

Other formats of content data are transferred as attachments along with SOAP message. Links to them are contained in the body. Attachments are encrypted and signed independently and the hash value for the signature is also entered into the body of the SOAP message. In addition to the actual content data, the SOAP body contains encryption and signature certificates from author and sender as well as encryption certificates of recipient and reader.

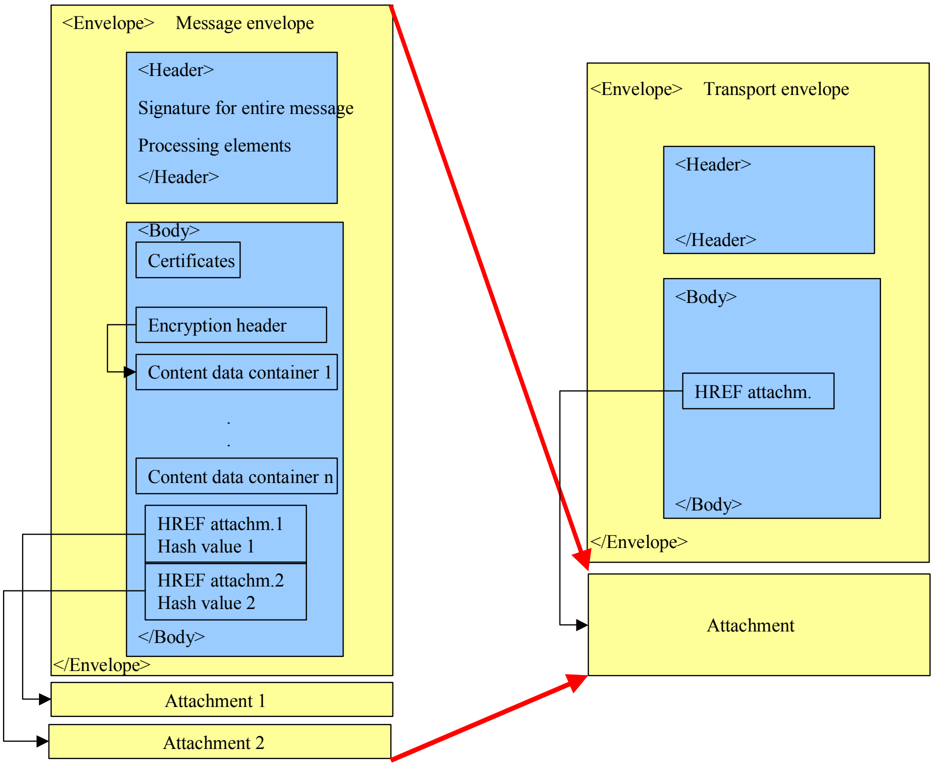


Figure 4: Structure of an OSCI packet

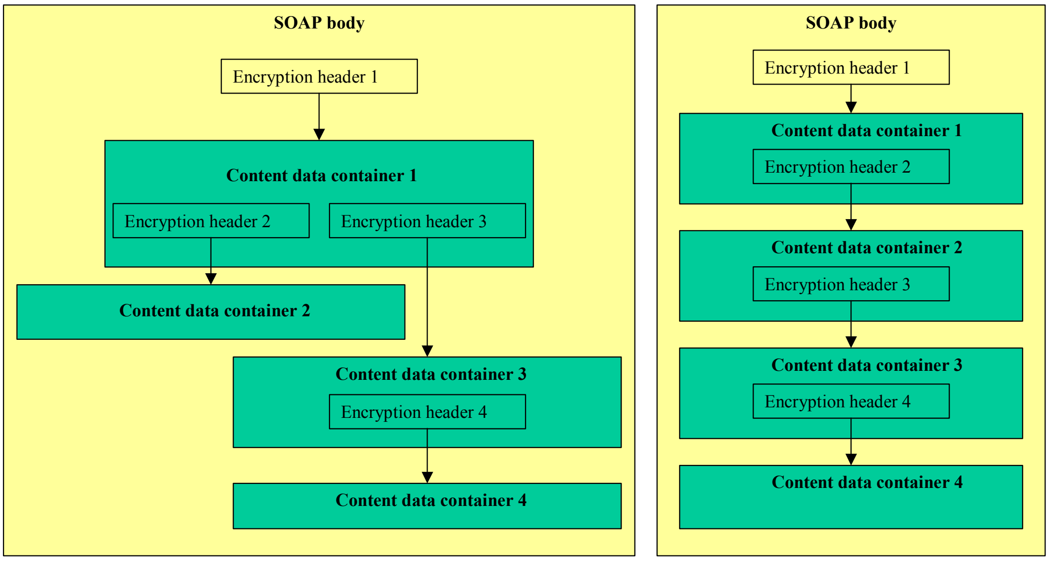
The header elements of the SOAP message contain the usage data (cf. chapter 3.2) which are required to process the message for delivery. In addition to providing an optional signature for the entire message, these header elements serve as process card for documenting and managing delivery and as a data object for monitoring the overall context of the dialog. The intermediary's signature and encryption certificate is also added in the header because it becomes a part of the message during the delivery process.

The exact layout of the SOAP document is determined by the type of message it contains. Transferring OSCI messages structured in this way is done by attaching it to another SOAP message that has a link to the original message in its body. The information required to optionally encrypt the usage data is found in the header of the second SOAP message.

Using the double-envelope principle ensures the integrity of the entire OSCI message during transfer, ruling out the possibility of attachments being tampered with. Instead of using a double envelope, this method allows other protocols such as SSL and S/MIME to be used for securely transporting data.

Each OSCI message has only one usage data container which is appended and updated by the recipient during the message delivery process. However, a message can contain more than one content data container each of which can be encrypted and signed separately. This makes it possible to address messages to different readers by encrypting the content data containers so that they can only be decrypted by the authorised reader.

There are additional advantages to using multiple content data containers. On the application level, rules on how the transferred content data are to be processed can be applied, i.e. rules are formulated for processing content data. A rules container holds the encryption headers required for decrypting additional containers. This ensures that the reader can read the other content data containers only after acknowledging the rules. This principle also allows a sequence for working through different content data containers to be determined.



3.2 Usage Data

Usage data primarily consist of the process card and the request for the intermediary on how to process the OSCI message. If required, the signature may be added to this.

The sender can encrypt the usage data using the intermediary's public key. This allows the data to be transported securely while permitting the intermediary to process them. The intermediary uses the public key of the sender to encrypt his responses (e.g. a receipt) to requests. This key is found on the process card of the request and can be used by the intermediary.

The process card controlling the processing of delivery requests remains the central data structure while the intermediary carries out processing and specifies the delivery modes and the level to which value-added services can be utilised. The intermediary generates the process card and updates it during the delivery process. The process card serves as a receipt for each communication partner and a copy can be requested from the intermediary. The delivery of a process card may also be signed by the intermediary.

The usage data have entries for all data fields required for transport:

- The authors' signature and encryption certificates
- The sender's signature and encryption certificates
- The reader's encryption certificate
- The recipient's encryption certificate
- Subject line
- Time stamp
- Processing status of the delivery request
- Elements for dialog control

Certificates establish the relationship between key pairs and sender/recipient and are based on the X.509, version 3 standard. Certificates contain the following items:

- Certificate owner name
- Period of certificate validity
- Issuing authority including certificate name
- Public key from the key pair
- Certificate type
- Signature of the certificate authority
- Certificate serial number

By adding entries to the process card it becomes a log of message transfers. If required, it can be provided as a receipt to either the sender or recipient. The intermediary can use process cards as a receipt of message transfers and their time of delivery.

Time stamps serve as general evidence that certain data passed through a time stamping service at a given time. A provisional Internet standard [PKIX-TSP 00] [1]covers this area and provides a general format for time stamp requests and their responses.

[1]requests to time stamping services can be unsigned or unsigned. In both cases the requests contain both the hash algorithm and the hash value of the digital data for which a time stamp is generated. However, signed time stamp request requests are transferred in encrypted form. Responses from time stamping services are always signed and encrypted.

The German Digital Signature Act does not stipulate that the time when the signature is generated must be evident in the signature; a signature without a time stamp also complies with legal requirements. Nevertheless, OSCI uses time stamps, not in the signature objects themselves, but on the process card instead. OSCI ensures that the time a document is signed closely approximates the time the intermediary makes an entry on the process card. The process card consequently provides a record not of the exact creation date but, instead, provides the nearly identical date of receipt as well as the transfer date. OSCI Transport 1.2 also provides for the use of accredited time stamps – these are time stamps from accredited trust centres. These are offered only as an option and are not absolutely required.

3.3 Content Data

Content data are composed of the actual business transaction data and, where present, the signature for the content data. Business transaction data may be file reference numbers, passwords on the application level for user authentication for the department involved as well as the initiator of the business transaction.

If required, content data can be encrypted using a reader's public key or the public keys of several readers, keeping the intermediary from viewing the data. This ensures that the data can only be read by the intended reader.

4. Security Risks

The entire OSCI Transport architecture is subject to the following basic threats:

- Loss of confidentiality – i.e. the danger posed by unauthorised persons gaining access to content and usage data.
- Loss of integrity – i.e. the danger that content and usage data are falsified while being transferred from the author/sender to the recipient.
- Loss of authenticity – i.e. the danger that content and usage data do not originate from the originator, author or sender.
- Repudiation of communication and authorship – i.e. the danger that the authorship, the transfer or the receipt of content or usage data is denied.
- Loss of availability – i.e. the danger that access to content and usage data or the OSCI system is unavailable, incomplete or too slow.
- Loss of traceability – i.e. the danger that an event cannot be (retroactively) traced back to an individual and a point in time.

These abstract concepts are so general in their nature that they do not sufficiently cover all the risks that the OSCI Transport architecture is subject to. The exact risks for each affected module must be ascertained.

The following section contains a complete discussion of the risk the intermediary's OSCI system, the user's backend system as well as the operating system of one of the communication partners is exposed to. All scenarios assume that unsecure transmission is used. But they also assume that the hardware or software of the sender or recipient has not been compromised.

The OSCI Transport architecture is exposed to the following overall security risks.

- **Working under a false identity:**

  A false identity can be assumed by using the ID of a legitimate user on the application level or by manipulating the network address.

  Anyone using a stolen identity can gain access to the OSCI system or one of its applications and access all data with the same rights as those assigned to the legitimate user. A stolen identity can be assumed using one of two methods:

  1. During user authentication an expired or invalid certificate is used to log in an invalid user. This can also be attempted by resending (encrypted) OSCI messages (replay attacks)
  2. After successfully logging in, the person assumes the ID of a different user permanently or for completing individual tasks. (Man-in-the-middle attacks)

  While having knowledge of confidential information or the possession of confidential materials is required for the first method and therefore is relatively independent of the technology being deployed, the second method relies on exploiting technical weaknesses in the system in use, where it is not able to securely manage information entered in the login routine.

  Manipulation of the network address on the transfer, network or transport layer level is not an issue for OSCI Transport, but instead concerns the administration of the OSCI system. This is discussed in detail in the OSCI operational concept document.

- **Gaining extended access rights:**

  If the assigned access rights are successfully extended, unauthorised manipulation of personal data can be carried out and confidential data accessed. Besides the possibility of gaining extended rights by working under an assumed identity, attempts may be made to gain additional rights under one's own user ID and then permanently assign extended rights which were initially assigned on a temporary basis only.

  This risk involves an attack by users with or without a certificate on the generally accessible OSCI Web server in an attempt to gain extended system rights. Additionally, administrators may attempt to misuse their admin rights.

  In terms of OSCI Transport 1.2, the resources requiring extra attention are those that are provided to individual communications partners, such as mailboxes.

- **Reading content data:**

  Content data can be intercepted by unauthorised users while being transferred or used. This may lead to confidential information being divulged to unauthorised individuals. There are two ways of intercepting data:

  1. Eavesdropping on the electromagnetic emanations of digital equipment: Electromagnetic emanations from screens, keyboards, printers and other peripheral devices can be tapped from certain distances and be analysed. This is one way of obtaining information about the data processed and access information. In most cases, however, electronic surveillance of this type is prohibitively complex.
  2. Eavesdropping on transmission media:

There is a hidden risk of unauthorised persons eavesdropping on data being transmitted across networks. In a broadcast-oriented network designed to exchange data among different users, internal staff can intercept all data being transferred. Outsiders can tap into any point along a communications line within or outside of a building. The effort required to accomplish this is largely dependent on the medium and its use. A special problem is posed by cases where eavesdropping has taken place without any sign providing evidence that it has occurred.

- **Reading usage data:**

  It's not just content data that can be tapped by unauthorised persons locally or while being transferred. There is also the risk of usage data being identified and reused in order to gain access to protected system resources. Usage data in OSCI Transport include information from the sender and recipient certificates which can also be used as non-disputable evidence of their exchanging a message.

  If it becomes possible to gain a substantial amount of usage data and analyse them, user profiles can be created and be used to the disadvantage of those affected without their knowledge. Usage data are available in considerable quantities to the intermediary.

- **Modifying content data:**

  The data can be modified by the author or sender locally or while being transferred to the recipient, although changing the data during transport requires a high level of authorisation to access the data transfer system as well as the appropriate know-how.

- **Modifying usage data:**

  If usage data are successfully modified, instances of communication exchanges can be contested both by the author and sender of a message as well as by the recipient. The point being contested can relate to the time when a message was sent or the time it was delivered.

  Permission to modify usage data can also be used to cover up the traces of manipulation to the content data so that it remains undetected.

- **Disrupting the system:**

  If the OSCI system is successfully disrupted, the service cannot continue to be made available to the required extent. This can lead to serious difficulties for scheduled delivery request commands.

  The OSCI system can be crippled by denial-of-service (DOS) attacks. During a DOS attack a large number of message packages are sent to the server, which then either ceases to work due to the overload or can no longer send feedbacks in the usual manner.

Given the risks described, the following section distinguishes between citizens with a valid certificate, administration, and intermediary as well as general users of the Internet, while citizens with a valid certificate and general Internet users can be distinguished by the way they access the system. General users of the Internet can usually attempt to break in to the system anonymously by breaching security without having access rights, whereas citizens at minimum have an advanced signature and use it to access sub-modules of the OSCI or backend system legally which can be later traced to that specific citizen.

Both citizens with a certificate as well as Internet users at large represent a serious threat even when there is only a minor security gap present because in this case unauthorised access to data amounts to a serious violation of data protection. On the other hand administrative personnel and the intermediary represent such a threat only in cases where confidential personal data become exposed. The operators of an intermediary service, however, normally have many more opportunities to exploit existing technological or organisational weak points. The following matrix shows the potential threat from each group of people.

Group of people **Security risks**	Citizen	Intermediary	Administration	Internet user
Working under a false identity	X	X	X	X
Gaining extended access rights	X	X	X	
Reading content data		X		X
Reading usage data				X
Modifying content data		X		X
Modifying usage data				X
Disrupting the system				X

5. Security Objectives

OSCI has a number of security objectives to reduce and/or avoid the security risks presented in section 4 above. OSCI Transport does not however cover each of these risks. Some of these risks involve the secure operation of the OSCI system and a secure client kernel; appropriate countermeasures are described in the OSCI operational concept document.

OSCI security objectives are presented in 5.1; In 5.2 the objectives not handled by OSCI are discussed.

5.1 OSCI Security Objectives

There are a total of five security objectives for OSCI Transport 1.2.

5.1.1 Confidentiality

OSCI allows both content and usage data to be transferred securely.

- Confidentiality of content data:
  OSCI provides encryption of the content data from sender to recipient and can thus guarantee the confidentiality of the content data while being transferred or while being processed by the intermediary.
- Confidentiality of usage data:
  Usage data can be sent encrypted from sender to intermediary and between intermediary and recipient. Usage data are read by the intermediary and appropriately appended.

With respect to the confidentiality of the content and usage data, the security priority levels *low* (no encryption) and *high to very high* (Triple-DES/AES encryption) are provided by OSCI. In other words, the effects when confidentiality has been breached may either be negligible or substantial or take on existential, threatening or catastrophic dimensions; the damage to the reputation of the administering body is considerable. Potential misuse of personal data can have grave consequences for a registered user's social and economic standing, possibly leading to financial and social ruin for the person affected.

5.1.2 Integrity

OSCI guarantees a manipulation-free transfer of both content and usage data.

- Integrity of content data:
  Content data can be signed by the author using his certificate or by several authors using their certificates. Falsifications can be detected only by the recipients.
- Integrity of usage data:
  Usage data is signed by the sender with his certificate. Falsifications are detected by the intermediary and the recipient.

With respect to the integrity of content and usage data, the security priority levels *low* (no encryption), *medium* (advanced signature) and *high to very high* (qualified/accredited signature) are provided by OSCI. In other words, the expected damage caused by the loss of integrity may be classified as low, medium or high to very high.

5.1.3 Authenticity

OSCI guarantees both user authentication (if a mailbox is being accessed or a receipt is being requested) and authentication of content and usage data. User authentication takes place during dialog initialization. During initialization a check is carried out to verify that the user is in possession of a private key assigned to the encryption certificate.

If user authentication is required (e.g. to allow access to mailboxes), the security priority levels *high to very high* (Triple-DES/AES) are provided by OSCI. In other words, the expected damage caused by invalid authentication may be classified as high to very high.

Data authentication refers to the authenticity of both content and usage data.

- Authenticity of content data:
  Content data can be signed by the author using his certificate or by several authors using their certificates. Reader/Readers verify the signature. The intermediary checks the validity of the certificate. If the content data transferred are authentic, they can be assigned to a person who possesses a valid certificate at the time the message is sent. For content data these are the author/authors. The authenticity is only detected by the reader.
- Authenticity of usage data:
  Usage data can be signed by the sender using his certificate. If the data are signed, the recipient verifies the signature. If the usage data transferred are authentic, they can be assigned to a person who possesses a valid certificate at the time the message is sent. For usage data this is the sender. Authenticity is detected by the intermediary or the recipient, respectively.

With respect to the authenticity of content and usage data, the security priority levels *low* (no encryption), *medium* (advanced signature) and *high to very high* (qualified/accredited signature) are provided by OSCI. In other words the expected damage caused by the loss of authenticity may be classified as low, medium or high to very high.

5.1.4 Non-Repudiation

Non-repudiation refers to both the authorship of the message and to the communications process.

- Non-repudiation of authorship:
  Non-repudiation of authorship is subject to requirements specified in the German Digital Signature Act. The German Digital Signature Act stipulates that qualified signatures must be used in cases where administrative law requires written records (cf. Appendix). The non-repudiation of having received a message is not ensured by OSCI.

  Non-repudiation of authorship is accomplished by signing content data and by archiving content data with the signature on the recipient side. If more than one author exists, they should each be able to sign the document. This requires multiple signatures.

  With respect to the non-repudiation of authorship, the security priority levels *low* (no encryption), *medium* (advanced signature) and *high to very high* (qualified/accredited signature) are provided by OSCI. In other words the expected damage caused by the lack of non-repudiation of authorship may be classified as low, medium or high to very high.
- Non-repudiation of the communications process:
  The non-repudiation of the communications process can be divided into two parts:
  - Non-repudiation of sending messages:
    Non-repudiation of sending messages ensures that the sender cannot successfully deny having sent a certain message.
  - Non-repudiation of message receipt:
    Non-repudiation of receiving messages ensures that the recipient cannot successfully

deny having received a message. The receipt of a message does not always automatically mean its contents have been read.

Non-repudiation of the communications process is accomplished by signing usage data and by archiving usage data with the signature (process card) on the intermediary side. On request, the intermediary can provide the communication partners with receipts for message delivery or dispatch.

In version 1.2, non-repudiation of receipt also refers to attachments, not only to the actual content data.

With respect to the non-repudiation of the communications process, the security priority levels *low* (no encryption), *medium* (advanced signature) and *high/very high* (qualified/accredited signature) are provided by OSCI. In other words the expected damage caused by the lack of non-repudiation of the communications process may be classified as low, medium or high to very high.

5.1.5 Traceability

Traceability is a combination of access control, record and log keeping as well as being able to track exact times.

- Access control:
  Access control prevents users and processes that are active for this user from obtaining read or write access to information and resources for which they have no authorisation, e.g. mailboxes and process cards.

  With respect to access control, the security priority level *high to very high* is provided by OSCI. In other words, the expected damage caused by the loss of access control may be classified as high to very high.

- Record and log keeping:
  Logs keep a record of all events, including any actions taken by unauthorised individuals.

  In terms of keeping records and logs, OSCI places this in the *high to very high* level of security, meaning that there is a high to very high risk posed by failing to keep security logs.

- Tracking of exact times:
  This is how the date and time a specific event occurred can be ascertained.

  In terms of tracking exact times, OSCI places this in the *low*, *medium* and *high to very high* level of security, meaning that the risk posed by failing to track exact times is *low* (no time log required), *medium* (insecure tracking of time is required) and *high to very high* (secure tracking of time is required).

The following table provides an overview of the levels of security that can be assigned to each security objective:

Confidentiality of content data	low		high to very high
Confidentiality of usage data	low		high to very high
Integrity of content data	low	medium	high to very high
Integrity of connection data	low	medium	
User authenticity			high to very high
Authenticity of content data	low	medium	high to very high
Authenticity of usage data	low	medium	
Non-repudiation of authorship	low	medium	high to very high
Non-repudiation of sending messages	low	medium	
Non-repudiation of message receipt	low	medium	
Access control			high to very high
Record and log keeping			high to very high
Tracking exact times	low	medium	high to very high

5.2 Security Objectives not Covered by OSCI

Identification of users and availability are not supported by OSCI. Other security risks (e.g. eavesdropping on the electromagnetic emanations of digital equipment) mentioned in section 4 are also not covered.

5.2.1 Availability

Content and usage data availability and overall system availability are primarily ensured by measures taken outside of OSCI. These are included in the operational concept.

5.2.2 User Identification

Digital signatures are closely related to signature certificates. This is a data format that matches a public key to the owner of a certificate. A certificate is only issued to individuals who can prove their identity by presenting personal identification.

Because someone has been issued a certificate does not mean that they are a form of digital identification that can be used in open systems to uniquely identify the owner without media discontinuities. In addition to information about the certificate (certificate no., period of validity), certificates based on the German Digital Signature Act contain at most the first and last name of the applicant. This does not provide enough information to uniquely identify an individual. There is still a risk that persons will assume the identity of another user to obtain illegitimate access to public administration departments. Cases of switched identities (e.g. two users having the same name) can later be settled because first and last names are signed with a unique key. But this is only of consequence for any later claims for damages; unauthorised access remains undetected.

In OSCI Transport 1.2, to uniquely identify an individual would require additional attribute certificates in fulfilment of § 7 (2) SigG (German Digital Signature Act). These certificates contain additional information about the certificate owner such as date and place of birth, etc. Attributes of this kind are not currently available on smart cards, meaning that the intermediary must be able to retrieve them (if it has not stored them locally) from the appropriate trust centre at any time. The user would still have to apply to the trust centre for the attribute certificates in advance. However, accessible attribute certificates stored at the certificate issuer are not yet in widespread use.

Because OSCI Transport cannot rely on the widespread use of attribute certificates, version 1.2 of OSCI Transport is designed to transfer information without prior identification of the sender. The only requirement for relaying messages is that the recipient is in the possession of a non-revoked encryption certificate because addressing takes place via this certificate. If the business transaction in question requires the message to be signed or encrypted, the sender must have access to the appropriate certificates.

However, the intermediary stillchecks the certificates. If the recipient's encryption certificate is revoked, the message is rejected. When a key has expired, the message is still delivered to the recipient, but he is given notification of the results in a check protocol (cf. 6.7).

OSCI Transport 1.2 does not recognise any users besides the intermediaries involved whose certificates are known to the client. Thus, OSCI Transport identifies no users, but instead assigns the transferred data to a unique certificate. In this sense, the information transferred can be considered authentic. Identifying communication partners is done on the application level.

6 OSCI Security Mechanisms

OSCI Transport 1.2 provides numerous mechanisms. Before describing the individual OSCI mechanisms in more detail, the following table can be referenced first to get an overview of how each individual mechanism is related to each security objective.

Security objectives **OSCI mechanism**		Confidentiality	Integrity	Authenticity	Non-repudiation	Traceability
A	Encryption of content data	high/very high				
B	Encryption of usage data	high/very high				
C	Decryption of content data	high/very high				
D	Decryption of usage data	high/very high				
E	Signing content data		medium high/very high	medium high/very high	medium high/very high	
F	Signing usage data		medium high/very high	medium high/very high	medium high/very high	
G	Verifying content data signatures		medium high/very high	medium high/very high	medium high/very high	
H	Verifying usage data signatures		medium high/very high	medium high/very high	medium high/very high	
I	Certificate check		high/very high	high/very high	high/very high	
K	Logging times					medium high/very high
L	Receipt mechanism				high/very high	
M	User authentication via dialog initialisation			high/very high		
N	Challenge-Response			high/very high		
O	Issuing and verifying message IDs			high/very high		

6.1 Encryption and Decryption of Content Data

On the business transaction level, content data can be encrypted or decrypted using a hybrid process. In this process, messages are encrypted using a symmetric Triple-DES or AES process, each session key is encrypted using the reader's public RSA key. The session key transferred is decrypted using the reader's private RSA key, the decrypted session key is used only to decrypt the actual message.

Users declare the algorithm in the encryption header and thus specify the process the intermediary is to use when handling the request . If the intermediary does not support the process selected by the user, the user is notified of this and the dialog is terminated.

This hybrid process allows documents to be sent encrypted to those acting on behalf of individuals or to multiple recipients (e.g. mailing lists). In this process the documents being sent are encrypted with a session key. This session key is sent RSA-encrypted to all recipients. It is irrelevant that all recipients can view the RSA-encrypted session key that is not intended for them.

Where encryption is used, in terms of content data confidentiality, encryption and decryption of content data is in the *high to very high* security level.

6.2 Encryption and Decryption of Usage Data

On the request level, a hybrid process can be used to encrypt usage data just like content data. On the way from sender to intermediary usage data are first encrypted and then decrypted after receipt because the intermediary requires read access to deliver the message or provide valued-added services. Usage data are once again encrypted by the intermediary before delivering the message to the actual recipient.

In terms of usage data confidentiality, encryption and decryption of usage data is in the *high to very high* security level.

6.3 Signing Content Data

Similar to encryption, documents are also signed using a hybrid process. Initially the hash values of all documents to be signed are combined into a single element. This element is then signed using RSA.

Users declare the signing algorithm in the signature header and thus specify the algorithm the intermediary is to use when handling the request . No OSCI participant – neither the user nor the intermediary – may modify the process while the dialog is active.

If the content data are formatted in XML, signed data are displayed in a suitable manner when being signed. Content data in other formats are not displayed when included as attachments with the actual message – only the file name and format of the attachment are given.

In OSCI data can be signed using the following types of signatures (cf. Appendix, section 2):

- Advanced signature
- Qualified signature
- Accredited signature

In terms of integrity, authenticity and non-repudiation of content data, signing content data is in the *medium* (advanced signature) and *high to very high* (qualified/accredited signature) security levels.

6.4 Signing Usage Data

Both content and usage data can be signed in order to ensure the authenticity and integrity of a document. Usage data are signed using the sender's signing key.

The intermediary only adds his advanced signature to usage data. The signature applied by the sender of a message can be advanced, qualified or accredited. Usage data do not have to be explicitly displayed while being signed.

In terms of integrity, authenticity and non-repudiation of usage data, signing these data is in the *medium* (advanced signature) and *high to very high* (qualified/accredited signature) security levels.

6.5 Verifying Content Data Signatures

After successful delivery of the OSCI message, it is in the best interest of the reader to validate the signature used to sign the content data. This cannot be done by the intermediary because the content data in the business transaction are encrypted. The signature verification and signing processes are essentially the same: The hash value is derived from the transferred document. In addition, the sender's public key is used to decode the digital signature contained in the signature header of the message transferred. If this value matches the calculated hash value, the document can be considered to be authentic and unaltered.

6.6 Verifying Usage Data Signatures

Usage data signatures are initially verified by the intermediary when receiving a message. The intermediary adds a process card to the usage data. This process card contains a record of signature verification results. If the signature cannot be verified, the message is not delivered, but is instead returned to the sender with notification that verification was unsuccessful. Updated usage data are then signed by the intermediary if required. The final recipient of the message verifies the signature that the intermediary used to sign the usage data. Signature verification is based on a process described in section 6.5.

6.7 Certificate Checks

In § 2 (3) SigG, a "qualified signature" is defined as a signature that refers to a certificate that was valid when the signature was created. In addition to verifying the signature mathematically (cf. 6.5), it is also necessary to check that the certificate was valid at the time the message signature was created. A certificate check requires the following steps:

- Mathematical verification of the certificate signature: The certificate's recalculated hash value must match the value obtained from the decrypted signature.
- Offline validity check: The time when validation is carried out falls within the validity period indicated on the certificate.
- Online validity check: The certificate has not been revoked at the time when validation is carried out.

As certificates constitute a part of usage data and can be accessed by the intermediary, it can verify the certificates for both content data and usage data. The same certificate may be used to sign both usage and content data if the author and sender are the same person.

The creation times for these two signatures may deviate in specific cases; however, this poses no problem if the signature for usage data refers to a valid certificate when the signature was created. Because a signature used to sign content data has a creation time that precedes the time a usage data signature is created, it can be assumed that the certificate was valid when the content data were signed.

If validation fails, this assumption cannot be made. If the usage data signature is based on a certificate that was not valid when the signature was generated, it cannot be assumed beyond doubt that the certificate was invalid when the content data signature was created. Theoretically, the certificate could have become invalid between the creation of the content data signature and the creation of the usage data signature. However, the recipient is always notified in cases where the certificate was invalid when the usage data signature was created. How the recipient deals with the invalid certificate – whether he authenticates the content data signature himself or refuses to accept the OSCI message – is up to him and may depend on the type of business transaction in question.

If the certificate is valid, the backend system is notified of its type (advanced, qualified or accredited signature). Verification results for each certificate are entered into a check protocol. If the recipient's encryption certificate has been revoked, the OSCI message is not delivered, but is instead returned to the sender with notification that verification failed.

6.8 Recording Times

The process card contains “sent” and “delivered” times entered by the intermediary. Optionally, the time of delivery can be entered using a signed time stamp. These time stamps are used for this:

- Advanced time stamp:
  This is issued by the intermediary and signed by him using an advanced digital signature.
- Qualified time stamp:
  This is created, signed and provided to the intermediary by an accredited trust centre.
- Accredited time stamp:
  This is created, signed and provided to the intermediary by an accredited trust centre.

The Digital Signature Act does not require that a signature's creation time be clearly indicated within a qualified digital signature. A signature complies with the act even without a time stamp. However, it is only possible to determine the exact time if the signature bears a qualified time stamp as set out in § 2 (14) SigG. If a qualified digital signature does not bear a qualified time stamp, any date shown refers to the system clock on the sender's environment. However, it is easy to manipulate the time on the system clock.

In terms of non-repudiation of message exchange, entering the time stamp is classified as requiring a *medium* (advanced time stamp) and *high to very high* (qualified/accredited time stamp) level of security.

6.9 Receipt Mechanisms

The process card serves as a receipt for sender, recipient and intermediary and can be requested by the intermediary in order to have proof of message dispatch or receipt. The process card also serves as a record of delivery for the intermediary.

The following requests and their responses can also serve as receipts:

The recipient confirms that he has received and carried out a request by sending a confirmation code in a response to the request.

The client confirms that he has received the response to the previous request by sending a request with a response value that matches the challenge value from the previous response and that has a message ID that is greater by one than the previous message ID.

Responses to fetch requests contain a repetition of the selection criteria given in the request and thus can also be used as receipts.

6.10 User Authentication within the Explicit Dialog Initialisation

When a dialog is initialised, a check is carried out to verify that the user is in possession of the private key assigned to the encryption certificate. A random number is encrypted with the user's public key and sent to the user who is being authenticated. If he is able to use his private key to correctly decrypt and return the encrypted value, he is then authenticated. This form of authentication is required to enable authorised access to mailboxes and to process cards. The owner uses his encryption certificate to gain access to mailboxes and process cards.

6.11 Challenge-Response Process

As previously mentioned, OSCI does not offer a method for identifying communication partners because this cannot be achieved with respect to an open user group. During a dialog, however, authentication takes place on the basis of a challenge/response process.

6.12 Issuing and Checking Message IDs

All OSCI packages delivered can have a message ID assigned to it, which is uniquely definite in terms of place and time all over the world. This message ID is then applicable to exactly one delivery from the sender via the intermediary to the recipient.

Message IDs are generated by the intermediary when requested by the sender. The intermediary checks if

- it has generated the message ID
- the message ID has never been used before

If this is not the case, the intermediary rejects the request contained in the sender's message. Issuing and verifying message IDs provides protection against replay attacks and double submission of messages.

Appendix: Legal Requirements for Electronic Business Connections

1. The New German Digital Signature Act

The act in effect since 22 May 2001 on the framework for digital signatures (SigG) has two objectives: It transposes to national law the EU directive in effect since 19 January 2000 on a common framework for digital signatures. The new German act also addresses the issues raised in an evaluation of the old signature act, as set out in the IuKDG (Information and Communication Services Act) report of the German federal government on 18 June 1999.

The new signature act is primarily concerned with the following changes:

- Regulating certificate authority liability
- Licensing of check offices
- Regulating the use of pseudonyms
- Regulating data protection in companies offering products and services using digital signatures
- More clearly differentiated signature terms
- Time stamp requirements
- Extending the scope of mandatory reporting for certificate authorities

2. Differentiated Signature Terms

An important component of the new German signature act is the differentiation between the following terms already found in the EU directive.

- Simple signature
- Advanced signature
- Qualified signature

Digital signatures are data in digital form for purposes of authentication. Initials or scanned signatures fall under this definition as well.

Additionally, **advanced digital signatures** must:

- be assigned exclusively to the owner of the signing key
- allow identification of the signing key holder
- be created by means which are under the sole control of the signing key holder
- be combined with the data in such a way that alterations to the data can be detected

Compared to advanced digital signatures, **qualified digital signatures** are created by a secure signature generation device and are based on a qualified certificate valid at the time the signature is generated which is only issued by certificate authorities (trust centres) to natural persons.

Additionally, one can speak of **accredited digital signatures** if the qualified signature has been issued by an accredited certificate authority.

The accredited signature is marked by

- a 30-year guarantee of verifiability (§15 (7) SigG)
- a comprehensive evaluation of all legally required technical products using state-of-the-art technology and science (§15 (8) SigG)
- state-supervised audits of certificate authorities prior to beginning operations (§15 (1) and (3) SigG)

However, for qualified signatures conforming to the EU directive for standard European signatures the following holds:

- qualified signatures do not guarantee permanent verifiability (§13 (1) and (2) SigG)
- limited evaluation of used technical components only (§17 (4) SigG)
- the certificate authorities must only report commencement of business to the state supervising body (§ 4 (1) and (3) SigG)

The German Digital Signature Act does not require that the time the signature was generated be indicated in the signature. A signature complies with the act even without a time stamp. However, it is only possible to determine the exact time if the signature bears a qualified time stamp as set out in § 2 (14) SigG.

3. Legal Validity of Digital Signatures

Official correspondence is subject to certain formal requirements. These include an official letterhead as well as the name of the office issuing the correspondence or of the official, closing with, among other things, a signature (with the exception of automated official notifications) as well as bearing a stamp or official seal, as the case may be. The outward form emphasises that the correspondence does not have to do with an individual but instead with an employee acting on behalf of an organisation.

Within the framework of electronic business transactions and legal relations, these requirements can be fulfilled with the aid of appropriate attributes. Not only can the person issuing the correspondence but also this person's commercial power of attorney for the organisation/government authority be recognisable and verifiable as far as possible in the text being transferred.

At what times signatures of a given quality are required is the subject of the *Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Formvorschriften an den modernen Rechtsgeschäftsverkehr (Act for Adopting Legal Forms in Civil Law and Other Formal Requirements to Modern Commerce)*. Expressly rejected is a practice which subjects electronic documents to the regulations concerning authenticity by official deeds because this would not do justice to the high evidentiary value of electronic documents bearing qualified signatures. The Act provides for introduction of § 126a for the BGB (German Civil Code) which would replace written form with electronic form provided the electronic document bears a qualified signature. Qualified signatures are thus to be used where previously written form had been legally required.

A comparable rule has also been embodied in administrative law. However, where official administrative acts no longer need to be documented in writing, the qualified signatures must be issued by accredited trust centres (accredited signature). The approval of electronic signatures in the court of law as called for in Art 5 of the EU directive is already accommodated by the general principle of law of free evaluation of evidence by the courts.

In cases of dispute, the quality of a signature is to be examined by one or more experts appointed by the court. An amended § 292a ZPO (German Civil Procedure Code) should make it easier for users of qualified electronic signatures (with or without accreditation the certificate authority) to prove their case by establishing a norm for prima facie evidence: *“Der Anschein der Echtheit einer in elektronischer Form (§ 126a BGB) vorliegenden Willenserklärung, der sich auf Grund einer Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.” (An elec-*

tronically signed declaration of intent provides – pursuant to the new section 126a of the German Civil Code – prima facie evidence for authenticity of authorship and content which may only be refuted by facts that make it seriously possible that the declaration was not given with the key holder's consent.) However, the fact that also qualified electronic signatures without accreditation of the certificate authority will benefit from § 292a ZPO is being criticised by many people.