OSCI – The secure communication standard for E-Government

The slogan "E-Government" refers to bundled processes that try, by using the new media, to make public administration services more efficient, productive and attractive for their customers.

The objectives of E-Government can only be reached if there is more extensive DP networking within administration; however, this should not become producer or product-dependent. Thus the need arises for a standard, that is defined by public administration - and not by the manufacturers.

The draft decisions for OSCI are based on the requirement for carrying out complete transactions between public administration and its customers using the Internet's channels on the E-Government portal. On behalf of public administration, the OSCI center is engaged in developing and reaching an understanding on the interoperable exchange formats required. The results of this work are to be utilized by public administration as a standard for those developing communal software.

This document deals with the following aspects:

(1) **OSCI functional requirements**
Which aspects are taken into consideration when developing OSCI?

(2) **Security objectives**
Which security objectives does OSCI pursue with these requirements?

(3) **The OSCI communication structure**
How are the requirements and security objectives implemented in the communication structure?

(4) **The role of the intermediary in the OSCI communication scenarios**
What central functions are assumed by the intermediary?

(5) **E-Government with OSCI**
Which aspects are taken into consideration when implementing E-Government using OSCI?

OSCI functional requirements

OSCI shows a scalable security architecture. When creating security measures, the OSCI center focuses on maximum requirements. We assume that it must be in the interests of public administration to be able to react to increased security requirements without having to carry out a fundamental re-structure of the security architecture.

The focus is on the mediated exchange of data with superior and maximum demands for integrity, authenticity and confidence as regards its content. The contents bear a qualified signature at the very least. During the transfer, a mediating location (intermediary) can perform surplus-value services without any infringement of confidentiality.

For this purpose a differentiation is made between the content data and utilization data.

and these are given a different form of encryption.The communication is symmetrical. Basically it is possible for both communicating partners to assume either the role of the sender or the recipient. The communication can be both synchronous and asynchronous - OSCI supports both possibilities. The OSCI delivery and collection orders ensure that messages can only be received by authorized recipients. Both the sender and the recipient of OSCI message data must be able to follow up the communication. A routing slip has therefore been introduced as an integral part of the utilization data on the order level.

The routing slip:

- controls the processing of the message to the intermediary
- defines the message modalities (also the data structures for time-stamps) and the use of the intermediary's surplus-value services
- is generated exclusively by the user and updated by the intermediary while processing the message.

Security objectives

The functional demands made on OSCI can be described with respect to the security objectives as follows:

Confidentiality

OSCI guarantees both the confidential transmission of the messages and their confidential storage with the intermediary. The intermediary does not gain any knowledge of the transported OSCI data content either, i.e. data concerning the respective business transaction.

Integrity and authenticity

The integrity and authenticity of the transported OSCI data are guaranteed by an electronic signature.

Obligation

Using the routing slip, the intermediary confirms by signature to the sender or recipient that he has sent, or received OSCI information data - and includes the date of delivery.

The OSCI communication structure

OSCI is a data-exchange format based on XML. The following is valid in each case for the data structure on the three security levels (administration, order and business transaction level):

- The data structure is a well-designed XML document;
- it is valid with respect to the given XML format.

The business transaction data level

This level contains the actual business transaction data. Its structure is modeled by special concepts adopted for implementing E-Government processes. The business transaction data is signed according to the "w3c digital signature“ standard.

The order level

The business transaction data is coded. The data necessary for decrypting on the receiving side is contained in the encryption header at order level. The routing slip is the central data structure that enables the intermediary to perform surplus-value services. In addition, the various certificates are found at the order level. Finally, the data at order level is similarly signed in order to guarantee the security objectives, user authentication and non-deniability. This signature is similarly applied in accordance with the "w3c digital signature“.

The administration level

The data at administration level is the only data that is sent between the respective communicating partners without any encoding or signature. It includes:

- the message header with data for securing the OSCI dialog;
- the sender's encryption certificate;
- and the decoding header required for decrypting at order level.

The role of the intermediary in the OSCI communication scenarios

The existence of a central mediating function, the so-called intermediary, that can provide surplus-value services without jeopardizing confidence on the business-transaction data level, is a characteristic feature for secure implementation of the E-Government processes using OSCI.

The intermediary thereby assumes the following tasks:

- Information is saved securely in an intermediate storage and only transmitted to authorized persons.
- Cryptographic functions that are cost and time-consuming can be centralized.
- The intermediary can check message delivery regulations.
- The intermediary is *the* safe administration portal
  Due to the encoding between the sender and the recipient, the intermediary is able to assume the role of a portal without causing any loss of confidentiality.

E-Government with OSCI

The general basic requirements for an infrastructure in which SigG-compliant transactions are possible, include the solution to the following issues:

- Key distribution
- Generation of messages

- Secure intermediary operations
- Certificate verification
- Backend adapter

When using OSCI for E-Government implementation, a differentiation is made between four different levels:

(1) Business transactions

On the business transactions level, the contents of E-Government transactions are transported. The data is usually in the form of XML data. Business transactions data is signed electronically by the sender, as a basic rule, in order to guarantee integrity and authenticity. Furthermore, the business transactions data generally contains confidential data; it is therefore coded between the sender and the recipient. To ensure the necessary security mechanisms, the basic OSCI functions are used.

(2) The basic OSCI functions:

The basic functions provide mechanisms that function independently of the transported content, in order to protect this content from any manipulation or unauthorized access. For securing the business transactions data, cryptographic OSCI measures are applied. From the perspective of the OSCI user, a particularly high demand for interoperability exists here, in order to ensure considerable independence in the choice of hardware and software options. OSCI therefore adopts standards such as W3C and ISIS MTT and BSI recommendations. The design of the basic OSCI functions is based on the German signatures law, "SigG". Besides the message structures for the security mechanisms with their content-independent design, the basic OSCI functions also comprise the exactly defined, OSCI-order types. These secure, for instance, the delivery and collection of messages using the respective means of authentication.

(3) The OSCI infrastructure:

The OSCI communication format is fully described by the two levels given above. In order to secure the implementation of E-Government processes one should, however, also bear in mind that OSCI business transaction data has to be generated by reliable applications. A further aspect entails distributing the communication-partner certificates in the public administration sector, where natural persons are not concerned. Theft of any data must also be prevented effectively. These measures do not constitute part of the OSCI specification. However, for an OSCI infrastructure of this type, the implementation

and distribution of applications in the form of signed Java applications is recommended. In addition, certificates belonging to communication partners who are not covered by the PKI (Public Key Infrastructur) in accordance with the SigG, are also distributed together with these applications.

(4) Products to be implemented

The measures described for the three preceding levels have to be implemented by means of specific products. In contrast to the other three levels, the competition here between the different products is certainly in the interests of the user. For this reason, OSCI has been disclosed as a standard. Public administration can make OSCI compatibility a standard for E-Government applications and products.

A differentiation must be made between the following main components:

- **OSCI kernels** encapsulate basic application-independent functions, in particular in the fields of cryptography and transport.
- **OSCI applications** perform individual applications and generate OSCI messages. They send them to the kernel for visualization, signature, encoding and transmission.
- The **OSCI intermediary** produces surplus value services without any loss of confidentiality and it manages the in-boxes of the users.
- **Backend adapters** integrate the special procedures existing in public administration into the OSCI infrastructure and thereby enable continued processing without any interruption in the media.

For further information please download the OSCI specification in its current version on our homepage http://www.bos-bremen.de.