

Glossary for Corporate eGateway

Corporate eGateway

Table of contents

1	<u>Introduction</u>	1
2	<u>Glossary</u>	1

Version change history

Version	Date	Description of changes
Version 1.2	2006-06-01	<ul style="list-style-type: none">▪ New abbreviations included▪ New lay-out of document
Version 1.3	2007-03-16	<ul style="list-style-type: none">▪ New definitions included (due to updated version of Corporate eGateway agreement)▪ New abbreviations included

Document title Glossary for Corporate eGateway
 Version 1.3
 Author
 Subject Glossary for Corporate eGateway
 – includes both business and
 technical abbreviations
 Department
 Project Corporate eGateway

2007-03-16 Date
 1(12) Page
 Reference

1 Introduction

The purpose of this document is to offer a glossary, for both business and technical use, of the important terms and descriptions used in connection with the Corporate eGateway service provided by the Nordea Group (hereinafter also referred to as Nordea). The descriptions and definitions listed in the table below are given in the context of the Corporate eGateway service and documentation thereof. Definitions used in either the Corporate eGateway agreements and/or described in this document are stated with capital letters throughout all the documentation related to the Corporate eGateway service.

The Corporate eGateway documentation is amended from time to time to reflect new requirements and functionalities of the service. The changes made to the documents might also effect the terminology used in the documents. Therefore the Glossary can also be used as a tool when comparing documents relating to Corporate eGateway including different terms and definitions. For instance, a Nordea customer, who has signed the version of the Corporate eGateway agreement called “Corporate EDI Gateway Agreement”, will be able to find in this Glossary the corresponding new terms used in said agreement. In case a customer is a SWIFTNet FileAct user, the customer will have signed the version of the Corporate eGateway Agreement for SWIFTNet FileAct users called “Corporate EDI Gateway Agreement for SWIFTNet FileAct users” and will also be able to find in this Glossary the corresponding new terms used in said agreement. (In connection to this please see the definition for “Present Customers”).

The document “Glossary for Corporate eGateway” can be found on the Nordea Group's homepage: www.nordea.com

2 Glossary

Term	Description
ACH	Abbreviation for automated clearinghouse. The ACH is a domestic multilateral clearing system to which the banks are connected. The banks often own the ACH, operating in the country in question. This type of domestic clearing system is used for low-value clearing/mass payments, that is non-urgent commercial payments such as supplier and salary payments.

Term	Description
Activity Plan	A document that may be used between the parties to the Testing Agreement to ensure a smooth and efficient Testing and implementation of the Service. The Activity Plan includes the project organisations for the parties to the Testing as well as a Test Timetable for the Testing and implementation of the Service. The Activity Plan is provided by Nordea.
Administrator	A natural person designated by the Customer in an Authorisation Document to administrate the Authentication Procedure on behalf of the Customer. Corresponding term for the Present Customers is “Authorised Administrator”.
Agreement	The Corporate eGateway agreement signed between the Customer and Nordea. If the Customer is a SWIFTNet FileAct user then the term “Agreement” refers to the Corporate eGateway agreement for SWIFTNet FileAct users signed between the Customer and Nordea. As concerns the Present Customers the term “Agreement” refers to the agreement version called “Corporate EDI Gateway Agreement” and in case the Present Customer is a SWIFTNet FileAct user to the agreement version called “Corporate EDI Gateway Agreement for SWIFTNet FileAct users”.
Authentication Procedure	An authentication technique and an authorisation procedure, including but not limited to the use of Means of Identification, and security measure, designated in the Service Specification Sheet and used in connection with the Service as described in the Service Documentation.
Authorisation Document	A power of attorney granted by the Customer substantially in a form as set out in Schedule 3 designating the Administrator(s) and the User(s).
AUTACK	<p>Recommended Practice for Message Flow and Security for EDIFACT Payments from UN/EDIFACT Finance Group SWG-F D6, 1998/99. A set of recommendations on how to implement financial EDIFACT Messages for a safe and effective exchange of financial information between financial institutions and their business customers.</p> <p>The AUTACK Message is used to authenticate and secure the complete interchange, one AUTACK per interchange conveying one or more digital signatures computed on the complete data of the entire interchange consisting of one or more messages.</p> <p>Corporate eGateway provides an interim security solution for syntax 3 message implementations, facilitating syntax version 4.</p>
AUTHOR	<p>Authorization message (EDIFACT message)</p> <p>Used in relation to Direct debiting for authorizing the Creditor to draw payments from the Debtor’s account</p> <p>Corporate eGateway has two versions of AUTHOR</p> <p>Corporate eGateway uses UN/EDIFACT directory D.96 A</p>
BBS	Account Clearing House in Norway (Bankenes Betalings Sentral). In some documents the term “Service Provider” is also used. See <i>Service Provider</i> and/or <i>ACH</i> .

Term	Description
BGC	Account Clearing House in Sweden (BankGiro Centralen). In some documents the term “Service Provider” is also used. See <i>Service Provider</i> and/or <i>ACH</i> .
BANSTA	Banking status message (EDIFACT message) The BANSTA message is used to report application errors. The message is used to report errors in the relationships between fields (e.g. a payment message specifies two remitters instead of a remitter and beneficiary), errors from checking a local database (e.g. daily credit limit exceeded or insufficient funds) etc. Such errors are reported by a ‘-ve BANSTA’ and indicate that the referenced message has been rejected. Corporate eGateway uses both +ve and -ve BANSTA. Corporate eGateway uses UN/EDIFACT directory D.96 A
Block Cipher	A symmetric cipher, which encrypts a message by breaking it down into blocks and encrypting each block.
Business Day	A day (other than Saturday, Sunday or other public holiday) on which banks are open for general banking business in the place or places necessary for any Nordea Company to carry out the Service.
Certificate	Contains a Public key, the owner’s profile information, an expiry date, the issuer’s distinguished name, the issuer’s signature and the certificate chain.
CIPHER	EDIFACT Container message for enciphered data. Fully encrypted EDIFACT Messages used for confidentiality purposes. Commonly used by corporations in the USA instead of AUTACK. Can be offered by Corporate eGateway.
Completion Date	A date agreed between the Customer and Nordea in the Testing Agreement by which the Testing must be carried out successfully.
CONFID	EDIFACT EAN Container message for enciphered data. Fully encrypted EDIFACT Messages used for confidentiality purposes. Can be offered by Corporate eGateway.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes. (ISO 7498-2)
Confidentiality of content	This solution protects the contents of a message/interchange against being read or exposed to unauthorised access. Protection can be achieved by encrypting the data. The message or transmission is essentially scrambled (e.g. substituting one character for another character) by the sender using an available algorithm and key, and decrypted or unscrambled by the receiver using the key and algorithm.
Contact List	A document containing the contact persons and contact information for both the Nordea Group and the Customer relating to Corporate eGateway. The Contact List is either an appendix to the Document “Guideline for Support”, or, as concerns the Present Customers, an appendix (Appendix B) to the Agreement.

Term	Description
Content integrity	This solution protects against the modification of the data exchanged. The sender can achieve this functionality by including an integrity control value within the interchange. This value is computed using an appropriate algorithm and secret key that is applied to the message once it is ready for transmission. The receiver applies the same algorithm using the sender's Public key (following the corresponding instructions) to the received message and the result must match the integrity value sent.
CONTRL	UN/EDIFACT Standard message, Syntax and service report message. This message is used as Control Message within Corporate eGateway whenever EDIFACT format is used. The CONTRL message is used to report functional acceptance (+ve CONTRL) or to report syntax errors (-ve CONTRL). The message is used to report errors in structure, errors in the format of fields (e.g. alpha characters in numeric fields, wrong format for dates etc.), errors in the UNZ, UNE and UNT control counts, etc. of messages and interchanges. It is not to be used for application errors, such as unknown account numbers, and it is not to be used for failed authentication. Corporate eGateway CONTRL messages is based on version 3 of ISO 9735 (EDIFACT syntax). See also <i>Control message</i> .
Control Message	Each electronic syntax and service report message in a form and substance as described in the Service Documentation and the Terms.
Corporate eGateway	Nordea Group's solution for host-to-host exchange of files in EDIFACT and/or other formats. Corresponding term for the Present Customers is "Corporate EDI Gateway".
CN	Corporate Netbank. The new browser-based portal solution for corporate customers.
CNA	Corporate Netbank. Administration. Browser-based solution for administration of CNcustomers: agreements, users, authorisation etc. Includes a mid-tier authorisation component that is used by other components to verify authorisation for users for specific actions. Not used by Corporate eGateway.
Cover Control	A check routine by the bank to ensure that sufficient funds are available on the debit account of the payment order instruction sent by the customer, in order to ensure a further processing of the instruction.
CREMUL	Multiple credit advice message (EDIFACT message) Corporate eGateway uses UN/EDIFACT directory D.96 A.
Customer	A company that has signed the Agreement or the Testing Agreement. Corresponding term for the Present Customers is "the Company".
Cut-off Times List	A document containing the cut-off times for Corporate eGateway.
Cryptography	The science of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge.

Term	Description
Data integrity	The property that data has not been altered or destroyed in an unauthorised manner. (ISO 7498-2)
Data origin authentication	The corroboration that the source of data received is as claimed. (ISO 7498-2)
DEBMUL	Multiple debit advice message (EDIFACT message) Corporate eGateway uses UN/EDIFACT directory D.96 A
DES (Data encryption Standard)	A secret key symmetric cryptosystem. It is an encryption block cipher defined and originally endorsed by the US government. DES operates on 64-bit blocks with a 56-bit key. It works well for encrypting a large set of data. (see also <i>Triple DES</i> .)
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and the integrity of the data unit and protect against forgery e.g. by the sender (ISO 7498-2)
DIRDEB	Direct Debit message (EDIFACT message) Corporate eGateway uses UN/EDIFACT directory D.96 A
Direct Debit	Direct Debit transaction or collection. An instruction from a creditor to ACH or Service Provider to debit a customer account and to credit own account.
Documents	The Agreement, including all Schedules and the Service Documentation, and each Power of Attorney.
EDI	Electronic Data Interchange. This definition is commonly used by most EDIFACT users worldwide. The definition may occur within any Corporate eGateway Service Documentation and is then primarily aimed towards those who use EDIFACT syntax format towards Corporate eGateway.
EDIFACT Message Format	Within EDI (in this case EDIFACT) a particular structured exchange of data is called a “message”. The term is used to describe a set of information elements, which are transmitted for performing a specific business or administrative function; these information elements are structured in such a way as to follow for their optimal transfer and handling by electronic means. A message thus consists of a number of segments structured in accordance with the ISO9735 syntax rules. See also <i>Message Format</i> .
Encryption	The transformation of data into a form unreadable by anyone without the corresponding secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the data.
Establishment Fee	A fee for the establishment of the Service paid by the Customer to Nordea upon request by Nordea.
Executing Bank	A Nordea Company, or subject to the Nordea Group’s approval any other bank providing a Local Service to the Customer and/or the Participating Company.

Term	Description
FIK	Transfer form in Denmark (Fælles IndbetalingsKort).
File Check	One of the first steps in the processing of a file upload. The file is checked for syntactical, semantic and duplicate errors.
File Conversion	The process of producing a new file in some file format based on a file in another format. The process might require that all information from the source can be meaningfully mapped to fields in the target file. The mapping might involve conversion of fields (like dates), patching of field lengths and computation of several source fields into one target field.
File Format	The definition of how information inside a file is to be structured (syntax) and how the information is to be interpreted (semantic). Examples of file formats: <ol style="list-style-type: none"> 1. CSV files - information separated by comma or semicolon 2. EDIFACT
File Transfer	<ol style="list-style-type: none"> 1. The ability to transfer files from a Customer's local file system to Corporate eGateway 2. The ability to transfer information from Corporate eGateway and save them as files in the Customer's local file system. <p>File transfers can be customer/user initiated or system initiated depending on the set-up at the customer.</p>
File Type	A specific category of files, e.g. <i>Payment File</i> . This term is used to describe a group of related files. The file type <i>is not</i> related one-to-one with a file format: <ol style="list-style-type: none"> 1. Specific instances of a given file type may have different formats 2. A format may be used for different file types <p>There can, however, be constraints - e.g. <i>some format</i> can only be used for payment files.</p>
FINCAN	Financial Cancellation Message (EDIFACT message) Corporate eGateway does not at present use FINCAN message for cancellation.
FINSTA	Financial statement of an account message (EDIFACT message) Corporate eGateway uses UN/EDIFACT directory D.96 A.
Four-Corner Model	The four-corner model defines the basic entities involved in the PKI. The four corners are the Subscribing Customer, Relying Customer, Issuing Participant and Relying Participant. Each entity or corner communicates only with one of its neighbours.

Term	Description
Hash function	<p>A one-way function, which maps a set of arbitrary strings of bits onto a set of fixed- length, strings of bits.</p> <p>A (mathematical) function, which maps values from a large (possibly very large) domain into a smaller range. A 'good' hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range. (ISO 9594-8)</p> <p>In a good hash function, small changes in the initial string lead to large changes in the end result.</p>
Hardware Security Module (HSM)	A networked hardware device that provides cryptographic services to authenticated entities.
Identrus	A company offering its member banks certification services and allowing them to offer interoperable services to their corporate clients in the B2B market. Identrus is regulated and audited by Federal Reserve. Identrus has a number of strategic partners, including SWIFT.
Interchange	Communication between partners in the form of a structured set of messages and service segments starting with an interchange control header and ending with an interchange control trailer (ISO 9735-1).
ISO	International Organisation for Standardisation
Key	A sequence of symbols that controls the operations of cryptographic transformation e.g. ISO/IEC 9798-1.
Key Management	The various processes that deal with the creation, distribution, authentication and storage of keys.
KID	Customer Identification in Norway (KundeIdentifikasjon)
KIR S.A	Direct debit service provider in Poland. The Direct Debit Service uses the electronic clearing service ELIXIR.
Local Service	A service provided by an Executing Bank and accessible through the Service.
MD 4, MD5	MD4 and MD5 are message-digest algorithms. They are meant for digital signature applications where a large message has to be "compressed" in a secure manner before being signed with the Private key.
Means of Identification	The means Users use to identify and authenticate themselves towards Nordea Companies and other Executing Banks, in accordance with the Authentication Procedure.
Message	<p>All data, sent in accordance with the Documents and the Terms, containing e.g. instructions (e.g. payment instructions), orders, messages, information (e.g. on account balances, outgoing and incoming payments and direct debiting) and all other communication, including but not limited to authentication data and Control Messages, sent in one or several files between the Customer and the Message Centre through the Service. Corresponding term for the Present Customers is "EDI Message".</p> <p>See also <i>Message Format</i>.</p>

Term	Description
Message Centre	The Nordea Group's data communication centre of the Service which, in accordance with the the Documents and the Terms, converts a Message received from the Customer to the appropriate local format for further transmission to the relevant Executing Bank or data received from the Executing Banks to the agreed Message Format for further transmission to the Customer. Corresponding term for the Present Customers is "EDI Centre".
Message Format	An electronic message format specified in the Service Specification Sheet. See also <i>Message</i> .
NDD	Nordea Direct Debit. A direct debit service for the whole Nordic area including Poland provided by Corporate eGateway.
Non-repudiation	The other party cannot deny his actions due to the neutrally recorded audit trail.
Non-repudiation of receipt	This security solution protects the sender of a message/interchange from the receiver's denial of having received the message. The sender must request an acknowledgement from the receiver that the message has been received. The receiver should include in the acknowledgement a digital signature based on the original message.
Nordea Bank Denmark	Nordea Bank Danmark A/S, Denmark, Copenhagen.
Nordea Bank Estonia	Nordea Bank Finland Plc, Estonia Branch, Estonia, Tallinn.
Nordea Bank Finland	Nordea Bank Finland Plc, Finland, Helsinki.
Nordea Bank Great Britain	Nordea Bank Finland Plc, London Branch, Great Britain, London.
Nordea Bank Germany	Nordea Bank Finland Plc, Niederlassung Deutschland, Germany Branch, Germany, Frankfurt.
Nordea Bank Latvia	Nordea Bank Finland Plc, Latvia Branch, Latvia, Riga.
Nordea Bank Lithuania	Nordea Bank Finland Plc, Lithuania Branch, Lithuania, Vilnus.
Nordea Bank Norway	Nordea Bank Norge ASA, Norge, Oslo.
Nordea Bank Poland	Nordea Bank Polska SA, Poland, Gdynia.
Nordea Bank Sweden	Nordea Bank AB (publ), Sweden, Stockholm.
Nordea Bank USA	Nordea Bank Finland Plc, New York Branch, USA, New York.
Nordea Company	A company or other legal entity within the Nordea Group. Corresponding term for the Present Customers is "Nordea Bank".
Nordea Group	Nordea Bank AB (publ), (registration number 516406-0120, Sweden) and all companies owned and/or controlled directly or indirectly by Nordea Bank AB (publ) at any given time.
Nordic	An entity used by Nordea Group, for keeping, storing, registration and

Term	Description
Processor/User Admin	maintaining the Authentication Procedure and/or User, including storages and maintenance of any Keys used in relation towards Corporate eGateway.
OCR	Optical Character Reading SE: Name of a payment service. NO: Name of a service reporting credit transactions DK: Name of identification on Transfer form (FIK)
Origin authentication	This solution protects the receiver against processing data from a party claiming to be another party, in other words, only message/interchange with valid authentication codes are processed. These authentication codes (e.g. message Authentication Code, MAC) are transmitted to the receiver, and the value depends on the content of the message and the algorithm applied to the message. The use of this solution additionally applies message integrity to the transmission.
Payment hotel	A function for storing payments sent by the customer prior to the payment date.
Participating Company	A company or other legal entity, which has granted a Power of Attorney and is thereby, represented by the Customer through the Service. Corresponding term for the Present Customers is "Account Holder".
Partner Bank	An Executing Bank not being a Nordea Company.
PBS	Account Clearing House in Denmark (Pengeinstitutternes BetalingsService). In some documents the term "Service Provider" is also used. See <i>Service Provider</i> and/or <i>ACH</i> .
PAYMUL	Multiple payment order message (EDIFACT message) Corporate eGateway uses UN/EDIFACT directory D.96 A.
PGP (Pretty Good Privacy)	PGP® or Pretty Good Privacy® is a cryptographic product that enables natural persons or companies to securely exchange messages, and to secure files with both <i>privacy</i> and <i>strong authentication</i> . Privacy means that only the intended recipient of a message can read it. Authentication identifies the origin of the information, gives certainty that it is authentic and that it has not been altered. This security method is offered by Corporate eGateway.
Power of Attorney	A power of attorney granted by a Participating Company substantially in a form as set out in Schedule 4, authorising the Customer to operate the Participating Company's Local Services designated in the power of attorney through the Service, in accordance with the Documents.
Present Customer	A customer of the Nordea Group that has signed the version of the Corporate eGateway agreement called "Corporate EDI Gateway Agreement" and appendices to it or in case of SWIFTNet FileAct a customer of the Nordea Group that has signed the version of the Corporate eGateway agreement called "Corporate EDI Gateway Agreement for SWIFTNet FileAct users" and appendices to it.
Private key	That key of an entity's asymmetric key pair which must normally (and

Term	Description
	essentially if non- repudiation is to work) only be known by that entity.
Public key	That key of an entity's asymmetric key pair, which can be made public.
Public Key Infrastructure (PKI)	An encryption method consisting of two keys. The same key cannot decrypt what it originally encrypted. This allows one to be distributed publicly and the other to be kept private. Not used by Corporate eGateway.
RSA	A Public key cryptosystem for both encryption and authentication.
Schedule 1	The Service Specification Sheet which is a schedule to the Agreement. Corresponding term for the Present Customers is "Appendix C".
Schedule 2	A document which contains a list of the Service Documentation and which is a schedule to the Agreement. Corresponding term for the Present Customers is "Appendix A".
Schedule 3	The Authorisation Document which is a schedule to the Agreement. Corresponding term for the Present Customers is "Appendix E". If the Present Customer is a SWIFTNet FileAct user the Authorisation Document may also include Appendix F and in this case the corresponding term is "Appendix E and F".
Schedule 4	The Power of Attorney, which is a schedule to the Agreement. Corresponding term for the Present Customers is "Appendix D".
Schedules	Schedules 1-4 to the Agreement. Corresponding term for the Present Customers is "Appendices" including all of the appendices to the Agreement.
Security Department	Nordea Bank AB's Security Department in Sweden responsible for the Authentication Procedure related to Corporate eGateway.
Service	Corporate eGateway service.
Semantic	The meaning and interpretation of some data.
Service Documentation	Documents (amended from time to time) listed in Schedule 2, containing information on, including but not limited to, the Service, the Local Services, the Authentication Procedure, the Message Format, the Message Centre, technical connections and the Service Support.
Service Provider	Could either be a local ACH institution operating the local low value transactions or a VAN supplier handling different communication matters for a company. See <i>ACH</i> and/or <i>VAN</i> .
Service Specification Sheet	A Document (amended from time to time) as set out in Schedule 1 designating, including but not limited to, the Message Format, the Authentication Procedure and the Local Services, used by the Customer in connection with the Service.
Service Support	A help desk that handles the inquiries of the Customer and the Participating Company concerning the Service. Corresponding term for the Present Customers is "Corporate EDI Gateway Support".
SHA-1	A hash function, Secure Hash Algorithm, which was originally published by U.S. National Institute of Standards and Technology in 1993.

Term	Description
SSL	Secure Socket Layer. Encryption standard for browser-based solution. Not used by Corporate eGateway.
Syntax	The structural requirements for the layout of some data.
SWIFTNet	SWIFT's IP-based messaging platform. It includes the core store-and-forward SWIFTNet FIN service and three additional messaging services: SWIFTNet InterAct, SWIFTNet FileAct, and SWIFTNet Browse. See also <i>SWIFTNet FileAct</i> .
SWIFTNet FileAct	A service allowing secure and reliable transfer of files and typically used to exchange batches of structured financial messages and large reports. SWIFTNet FileAct supports tailored solutions for market infrastructure communities, closed user groups and financial institutions.
SWIFTNet FileAct user	Customer using Corporate eGateway service through SWIFTNet FileAct and, by that, enabling SWIFTNet's own security standard as described in the documents "Security and Communication Description for SWIFTNet FileAct", "SWIFTNet FileAct Service Operations Guide" and "SWIFTNet Public Key Infrastructure – Product Overview".
Terms	The terms and conditions of the Agreement.
Test Timetable	A timetable for the Testing as set out in the Activity Plan.
Testing	The testing of the Service during which the Customer and relevant Nordea Companies will test the Service. For example by sending messages to each other in order to see to that the Customer's enterprise resource planning ("ERP") system is set up and implemented in a proper way, and that the result and response are as expected, but also to ensure a proper communication set-up between the parties involved in the Testing.
Testing Agreement	An agreement where the Customer and the Nordea Group have agreed on testing Corporate eGateway.
Triple DES	A variant of DES, which operates on a block of data, three times with two or three keys. There are a number of different triple encryption methods, the most common one (with two keys) is where the data is encrypted with the first key, the result is decrypted with the second key, and the result of that is encrypted with the first key. This is sometimes called Encrypt-Decrypt-Encrypt (EDE) mode.
TrustAct	A service by SWIFT to provide trusted electronic messaging. The identity proofing and encryption is currently done with Identrus PKI's. TrustAct allows time stamping and storage of messages. Payments over open Internet have been designed. Additional services are to be launched shortly.
User	A natural person representing the Customer and the Participating Company through the Service (or otherwise in connection with the Service) in relation to the Local Services according to the Authorisation Document. Corresponding term for the Present Customers is "Authorised User".

Term	Description
VAN	Value Added Network. Suppliers that facilitate <u>EDI</u> , moving data from one company to other companies or provide other network services between one or several EDI users. VAN providers nowadays focus mostly on offering EDI translation, <u>encryption</u> , secure e-mail, management reporting, and other extra services for their customers.
VPN	VPN (Virtual Private Network) is a secure way of setting up communication between two points over the Internet. A so-called tunnel is established between the points. This tunnel consists of encrypted information that only can be decrypted by the other point.
X.400	A communication protocol, mostly used by large companies. All large telecom companies provide this protocol and they are also connected to one another under special branch organisations. Communication protocol used by Corporate eGateway.
XML (eXtensible Mark-up Language)	Syntax originally used for transporting inventory data, but later extended to cover a wide range of services, such as financial data. A cross-platform, extensible, and text-based standard for representing data. Also a key technology in the development of Web services. XML is for the time being not offered as a Message Format towards Corporate eGateway.