

CEN

CWA 16036

WORKSHOP

November 2009

AGREEMENT

ICS 35.040; 35.240.01

English version

Cyber-Identity - Unique Identification Systems For Organizations and Parts Thereof

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Foreword	4
Introduction.....	5
1. Scope	6
2. Normative References.....	7
3. Definitions And Abbreviations	8
3.1. Definitions.....	8
3.2. Abbreviations.....	10
4. Part 1: Collection Of Requirements	13
4.1. Taxonomy Of Identification Schemes.....	13
4.1.1 Introduction.....	13
4.1.2 ISO/IEC 6523: Structure For The Identification Of Organizations And Organization Parts 15	
4.1.3 Overview Of Types Of Business Identification Schemes.....	15
4.2. Questionnaire For Issuers Of Unique Identifiers.....	29
5. Part 2: Inventory Of Applications And Associated Requirements.....	32
5.1. List Of Application Areas.....	32
Table 1 - Assessment of Application Areas With Regards To Identification Schemes.....	32
5.2. Meta-Identification Schemes.....	34
5.2.1 Introduction.....	34
5.2.2 Inventory.....	34
5.2.3 Interoperability	35
5.2.4 Mapping.....	36
5.2.5 Requirements And Recommendations.....	37
5.3. Verification Of Identifiers In Registries	38
5.3.1 Registration Criteria	38
5.3.2 Recommendations.....	39
5.4. Resolution Interfaces/Protocols And Services.....	39
5.4.1 Overview.....	39
5.4.2 Domain Name System (DNS) Based Systems.....	40
5.4.3 Hypertext Transfer Protocol (Secure) - HTTP(S) Based Systems	40
5.4.4 Lightweight Directory Access Protocol (Secure) - LDAP(S) Based Systems	41
5.4.5 SOAP And ebXML Messaging Services (ebMS) Based Systems	41
5.4.6 Comparison Of Different Protocols.....	41
5.4.7 Specific Applications.....	42
5.4.8 Community Of Resolution Services.....	43
5.4.9 Technical Security Criteria	44
5.4.10 Requirements And Recommendations	45
6. Part 3: Use Cases And Specific Issues.....	46
6.1. Technologies In Use	46
6.1.1 Introduction.....	46
6.1.2 URI	46
6.1.3 IRI.....	47

6.1.4	PKI.....	47
6.1.5	UN/EDIFACT	50
6.1.6	UBL And GENERICODE	50
6.1.7	ebXML	51
6.1.8	OpenSearch	52
6.2.	Use Cases	52
6.2.1	Introduction.....	52
6.2.2	X.509 Public-Key And Attribute Certificates	53
6.2.3	eInvoicing	54
6.2.4	UBL	55
6.2.5	ebXML Messages / ebXML CPPA	55
6.2.6	UN/EDIFACT And According Transport Mechanisms	56
6.2.7	Trustlabels	57
6.2.8	Presentment Of Conformity Assessment Certificates.....	58
6.2.9	Usage In Registered Mail And Similar Systems	59
6.3.	Legal Considerations	61
6.3.1	Legal Effect Of Identifiers.....	61
6.3.2	Liability Of Providers.....	62
6.3.3	Governance Issues.....	62
6.3.4	IPR Issues	63
6.3.5	Policy Requirements.....	63
6.4.	Conclusions	63
Annex A (Informative)	Background Information.....	66
A.1	PKI.....	66
A.2	eInvoicing	69
Annex B (Informative)	Questionnaire For Issuers Of Unique Identifiers	70
B.1	Overview.....	70
B.2	Questionnaire	70
B.3	Analysis of the replies	75
Annex C (Normative)	Summary Of Recommendations	85

Foreword

The production of this CWA (CEN Workshop Agreement) specifying “Cyber Identity: Unique identification systems for organizations and parts thereof” was formally accepted at the Workshop Cyber ID kick-off meeting on 11 April 2008.

This CWA consists of three main chapters (parts):

- Collection of requirements
- Inventory of applications and associated requirements
- Use cases and specific issues

The document has been developed through the collaboration of a number of contributing partners in the Workshop.

The CWA approval was obtained following an electronic approval process that finished on 5th October 2009. The following organizations express their support to the CWA:

GS1 Europe

GS1 Switzerland

ID Partners (France)

Bernard Istasse consultant (France)

Athens Chamber of Commerce (Greece)

Dr. Otto Müller Consulting (Switzerland)

ENISA (European Network and Information Security Agency)

Multicert (Portugal)

The Federal Authorities of the Swiss Confederation, Federal Strategy Unit for IT (FSUIT), (Switzerland)

Odette (UK)

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN : AENOR, AFNOR, ASRO, BDS, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN Management Centre.

Introduction

Nowadays private and public organizations are increasingly relying more on electronic means of communications for carrying out their daily transactions for eBusiness and eGovernment purposes.

In electronic communications, to gain the trust and confidence of transacting parties, a required element is certainty regarding the organizations involved. Knowing exactly which the acting organization actually is, has become a matter of paramount importance for all transacting parties. This issue is known as “Cyber-Identity”. The matter is often reduced to secure authentication, but goes far beyond this limited subject. Reliable business information stored in trustworthy registries (official commercial registries as well as privately owned and operated directories) accessible online are another part of the picture which is often neglected.

Furthermore, regulations to fight against cyber criminality will enforce traceability of transactions, e.g. “know your customer” principle or anti-money laundering regulations. These examples show that the topic of the Workshop is also a cornerstone of the IT Governance.

Unique persistent identification of business entities by recognised bodies and the verification of such identifications in trustworthy registers are a prerequisite for interoperability in open user groups e.g. standards for electronic business exchange may mandate the use of unique identifiers in certain fields but do not specify how they can be decoded and resolved without a bilateral agreement. Therefore, the purpose of this CWA is to discuss these issues and provide standardisation bodies with proper recommendations to achieve this goal.

Several business registries currently in place address the issue of business Cyber-Identity albeit in a non-uniform manner. A significant amount of resources remains untapped, due to incompatible and non-interoperable business registries that mainly operate in isolation within non interoperable application domains.

The targets of this CWA are also in line with the EC Communication i2010 of the European Commission which indicates interoperability as a main challenge for creating a single information space and identity management as one area for action.

1. Scope

The present document gives guidance on unique identification systems currently in use or emerging for organizations and parts thereof. This covers organizational and operational rules and processes to enable interoperability across multiple organization identification schemes. Stress is laid on the persistence or permanence of the identification, i.e. that an according identifier designates the same entity over a long period. It comprehends an analysis of existing systems and proposes recommendations on how to achieve interoperability among them by using meta-identification systems. These specifications form an umbrella over disparate schemes for business directory services in order to create a reconciled and workable framework that can be used in multiple application environments. The focus is on unique identification systems used in Europe taking into account relevant international standardisation developments.

The document concentrates on the usage of unique identifiers in “open” systems and user groups. The borders between open and closed groups are fluent and closed groups may be integrated in open groups at a later stage. Stress is laid on identifiers used in open exchange and which can be verified in directories accessible over the Internet. However, identification of products which are consumer goods is not in the focus of this document. In particular, this CWA focuses on the following topics:

- **Organization identification schemes** which allow to identify the organization; Including schemes which allow to identify the organization and organization parts (e.g. organizational units, establishments, documents or services provided by the identified organization – see “organization part” in “Definitions”), thus any relevant entity which can be identified uniquely.
- **Verification of the identified organization contained** in such a scheme and registered **in a directory service**. Special consideration is given to governance issues and legal considerations concerning the registers as well as how secure access is ensured to such registers.
- **Bringing together various schemes** without obligating the scheme issuers to change their registration process.

The document contains an analysis of architectural models of interoperability of directories and resolution services and gives recommendations in order to assure low administrative effort and a maximum flexibility of using organization identification schemes and of verifying identifiers.

For the purpose of this Workshop, the term “Cyber-Identity” is restricted to worldwide unique identification of business entities and parts thereof by applying unique identifiers and “verification” solely to verifying the identified organizations by using a publicly available directory/register for organizations/companies. Excluded from the scope of this CWA is identification of citizens and consumers, although it will be taken into consideration that some issues are common to identification of citizens and consumers and an interface might be needed in future.

International standards covering issues addressing identification systems of organizations are taken as reference for the present document.

2. Normative References

Normative References

CA/Browser Forum “Guidelines for the issuance and management of Extended Validation Certificates” Version 1.2

ISO/IEC 6523-1, Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes

ISO/IEC 6523-2, Information technology — Structure for the identification of organizations and organization parts — Part 2: Registration of organization identification schemes

ISO 7372, Trade data interchange -- Trade data elements directory

ISO/IEC 9834-1, Information technology -- Open Systems Interconnection -- Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree

ISO/IEC 15459, *Information technology - Unique identifiers*

ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems – Requirements

ISO/IEC 27002, Information technology -- Security techniques -- Code of practice for information security managements

IETF RFC 1737 “Functional Requirements for Uniform Resource Names”

IETF RFC 2141 “URN Syntax”

IETF RFC 2396 “Uniform Resource Identifiers (URI): Generic Syntax”

IETF RFC 2616 “Hypertext Transfer Protocol -- HTTP/1.1”

IETF RFC 3406 “URN Namespace Definition Mechanisms”

IETF RFC 3987 “Internationalized Resource Identifiers (IRIs)”

IETF RFC 4043 Internet X.509 Public Key Infrastructure - Permanent Identifier

IETF RFC 4130 “MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)”

IETF RFC 5024 “ODETTE File Transfer Protocol 2”

OpenSearch 1.1 specification of OpenSearch.org

W3C HTML 4.01 Specification

W3C XHTML™ 1.0 The Extensible HyperText Markup Language

W3C Extensible Markup Language (XML) 1.0

X.509, ITU-T Rec X.509 | ISO/IEC 9594-8: 2005: “Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks”

X.520, ITU-T Rec X.520 | ISO/IEC 9594-6: 2005: “Information technology -- Open Systems Interconnection -- The Directory: Selected attribute types”

3. Definitions And Abbreviations

3.1. Definitions

For the purposes of this document, the following terms and definitions apply:

3.1.1 Abstract Syntax Notation One (ASN.1): ASN.1 is a flexible standard for the platform independent description of data structures. ASN.1 is specified in ISO/IEC 8824 / ITU-T X.680 series.

3.1.2 Basic Encoding Rules (BER): The BER are one way to binary encode (and compress to a certain extent) *ASN.1* messages. BER is specified within the *ASN.1* specification in ISO/IEC 8824 / ITU-T X.680 series.

3.1.3 Community of resolution services: Within this document this term denotes standards of operation that allow sharing of data of multiple, independent, self-governing providers without affecting their applications.

3.1.4 Data element: A unit of data for which the definition, identification, representation and permissible values are specified by means of a set of attributes (ISO/IEC 11179-3).

3.1.5 Directory: A business directory, i.e. database of organizations, parts thereof and any kind of related attributes and documents. The terms directory, register and registry are used as synonyms within this document.

3.1.6 Domain Name System (DNS): The DNS is a hierarchical naming mechanism and the basis for domain names which are widely used in the Internet. It is specified in RFC 1034 and RFC 1035.

3.1.7 Federation: See *Community of resolution services*

3.1.8 Identifier: A character or group of characters constituting a *data element* value used to identify or name an object and possibly to indicate certain properties of that object. (ISO/IEC 6523-1)

3.1.9 Identification scheme: A system allocating *identifiers* to registered objects. (ISO/IEC 6523-1)

3.1.10 Issuing Organization: A body that assumes responsibility for the administration of a specific identification scheme.

3.1.11 Lightweight Directory Access Protocol (LDAP): LDAP is a protocol for directory operations (query and modify) over TCP/IP. It is specified in RFC 4510.

3.1.12 Meta-Identifier: An *identifier* used to identify an *identification scheme*.

3.1.13 Organization: A unique framework of authority within which a person or persons act, or are designated to act, towards some purpose. (ISO/IEC 6523-1)

3.1.14 Organization identification scheme: An *identification scheme* dedicated to the unique identification of *organizations*. (ISO/IEC 6523-1)

3.1.15 Organization identifier: The identifier assigned to an organization within an organization identification scheme, and unique within that scheme. (ISO/IEC 6523-1)

3.1.16 Organization part: Any department, service or other entity within an *organization*, which needs to be identified for information interchange. (ISO/IEC 6523-1)

3.1.17 Register or Registry: See directory.

3.1.18 Resolution service: A service that can resolve unique identifiers to retrieve the associated attributes. The resolution may be performed by looking the identifier up in a directory/register or by redirection to another resolution service.

3.1.19 SOAP: SOAP is an XML-based protocol for the exchange of structured data, i.e. in so called "Web-Services". SOAP is the cornerstone of the *Web-Services protocol Stack (WS-*)*. The SOAP specification is available from the XML Protocol Working Group of the World Wide Web Consortium (W3C).

3.1.20 Secure Socket Layer (SSL): SSL is a security protocol that was developed by Netscape. It is the predecessor of *Transport Layer Security (TLS)*.

3.1.21 Straight Through Processing (STP): STP stands for the automated end-to-end processing of data without manual intervention (in the financial sector).

3.1.22 Transport Layer Security (TLS): TLS is a protocol in the TCP/IP-suite that runs on top of a reliable transport-layer protocol. TLS provides encryption, authenticity and integrity of a connection. TLS is specified in RFC 5246.

3.1.23 Transmission Control Protocol (TCP): TCP is a protocol in the transport layer of the TCP/IP-suite that provides a reliable exchange of messages with error-checking. TCP is specified in several RFC documents, the roadmap can be found in RFC 4614.

3.1.24 Trusted Third Party (TTP): A Trusted Third Party facilitates interactions between two parties who both trust another ("a third") party. This does usually not imply a direct involvement of TTP's in such a transaction. Bodies that enjoy confidence in the physical world can also act as TTP's in the electronic world.

3.1.25 Web-Services protocol Stack (WS-*): WS-* is a protocol suite for the implementation of so called "Web-Services". It includes the *SOAP*-protocol.

3.1.26 User Datagram Protocol (UDP): UDP is a protocol in the transport layer of the TCP/IP-suite that provides a fast but not reliable exchange of messages. UDP is specified in RFC 768.

3.2. Abbreviations

ABN	Australian Business Number
ACN	Australian Company Number
AML	Anti-Money Laundering
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
AS2	Applicability Statement 2
ATS	Alternative Trading System
BBAN	Basic Bank Account Number
BER	Basic Encoding Rules
BIC	Bank Identifier Codes
BRITE	Business Register Interoperability Throughout Europe
BSI	British Standards Institution
CA	Certification Authority
Crefo	Creditreform
CIS	Commonwealth of Independent States
CSD	Central Securities Depository
CSP	Certification Service Provider
D&B	Dun & Bradstreet
DN	Distinguished Name
DNS	Domain Name System
DNSSec	Domain Name System Security Extensions
DUNS/D-U-N-S	Data Universal Numbering System
EANCOM	EAN(GS1)+Communication
EasyNumber	Enterprise Access System Number
ebMS	ebXML Messaging Services
EBR	European Business Register
ebXML	Electronic Business using XML
ebXML CPPA	ebXML Collaborative Partner Profile Agreement
ECN	Electronic Communication Network
EDI	Electronic Data Interchange
EV	Extended Validation
G2G	Government to Government
GEPIR	Global Electronic Party Information Register
GLN	Global Location Number

GS1	Global Standards One
IANA	Internet Assigned Numbers Authority
IBAN	International Bank Account Number
IBEI	Identification of Business Entities Identifier
ICD	International Code Designator
INSEE	Institut National de la Statistique et des Études Économiques
IO	Issuing Organization
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IBAN	International Bank Account Number
IBEI	International Business Entity Identifier
ICD	International Code Designator
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INSEE	Institut National de la Statistique et des Etudes Economiques
IRI	Internationalized Resource Identifier
ISIN	International Securities Identification Number
ISO	International Organization for Standardization
KYC	Know Your Client/Customer
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
MiFID	Markets in Financial Instruments Directive
MTF	Multi Trading Facility
NACE	Nomenclature d'Activités Européenne
NAFTA	North American Free Trade Agreement
NID	Namespace Identifier
OASIS	Organization for the Advancement of Structured Information Standards
OFTP	Odette File Transfer Protocol
OI	Organization Identifier
OID	Object Identifier
OPI	Organization Part Identifier
OSCAR	Odette System of Coding and Registration
OSI	Open Systems Interconnection (Model)
PDF	Portable Document Format
PEPPOL	Pan-European Public eProcurement On-Line
PKI	Public Key Infrastructure

RCS	Registre du Commerce et des Sociétés
RDF	Resource Description Framework
REID	Registered Entity IDentifier
REM	Registered E-Mail
REST	Representational State Transfer
RFC	Request For Comment
SEPA	Single Euro Payments Area
SIREN	Système d'Identification du Répertoire des ENtreprises
SIRENE	Système Informatique pour le Répertoire des ENtreprises et de leurs Établissements
SIRET	Système d'Identification du Répertoire des ETablissements
SME	Small and Medium-sized Enterprise
S/MIME	Secure / Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
STP	Straight Through Processing
SWIFT	The Society for Worldwide Interbank Financial Telecommunication
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTP	Trusted Third Party
UBL	Universal Business Language
UCS	Universal Character Set
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UN/EDIFACT	United Nations Electronic Data Interchange For Administration, Commerce, and Transport
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VAN	Value Added Network
VAT	Value Added Tax
VCD	Virtual Company Dossier
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language

4. Part 1: Collection Of Requirements

4.1. Taxonomy Of Identification Schemes

4.1.1 Introduction

General Market Trends Of Identification Schemes

Different approaches shall be taken into consideration when talking about company identifiers. On one side stands the approach of standards¹ organizations with a long term vision and the capability to implement additional IT functions, on the other side the approach of industry driven² identifiers. In between, specific industries have promoted identification systems to meet their particular needs³ and a willingness to facilitate trade between business partners. In parallel to standardisation and finance initiatives, each country operates its own identification scheme⁴ to manage its relationships with its tax administration entities. Finally, the EU has recognised the role of VAT numbering, whose primary purpose is to facilitate tax refund across the Member States.

None of these claims for a unified approach or to replace the other, but one shall take into account the history of each of them and how they complement for specific business purposes. Standardisation bodies have set up rules for the wide identification of companies under the responsibility of ISO, the International Standardisation Organization. Industry sectors have promoted identifier systems to facilitate searches and provide a means for ascertaining the trust between business partners.

If international standards have been less popular at their inception, as they don't offer search capabilities, they are receiving an increased recognition as they provide powerful fund transfer functions which directly meet the capabilities of IT system and very soon the SEPA principles. In addition, they benefit tools and control capabilities which can fulfil security requirements such as KYC and AML principles. Finally, there is an increasing demand for Machine to Machine protocols in various business activities; procurement, supply chain, fund transfers etc., which require to rely on stable company identifiers rather than sectoral identification systems.

It is worth recalling that the EC has supported various initiatives to federate existing systems; back in 1995, EDIRA⁵ already aimed at coordinating EDI compliant companies under a common Registration Authority. Launched more recently, the BRITE⁶ project aims to develop inter-registry compatibility. The concept is based on a virtual network of heterogeneous registries that would be made compatible over the Internet "This initiative is not however an effort to replace other identification systems. What it proposes is a codification of a classification system for things that already exist"⁷, all of them being managed by a central directory. As a specific task, the BRITE

1 (ISIN, BIC, MIC...)

2 (D-U-N-S, EasyNumber, Crefo)

3 (e.g a GLN in case of location identification)

4 eg. Company registry or EBR at the EU level <http://www.ebr.org/>

5 The EDIRA System was developed, under sanction of the European Commission, in cooperation with several European Chambers and International Organizations experienced in the subject of "Electronic Commerce", in the context of the TEDIS European Program. The EDIRA System has succeeded in coordinating the coexistence and compatibility of a variety of "Identity Codification Schemes", used by various EDI participants, while simultaneously defining the rules for the harmonious co-operation of EDIRA Registries.

6 BRITE (www.briteproject.net) is the acronym for "Business Register Interoperability Throughout Europe". It is an EU Commission funded research project on the establishment of links between Business Registers. BRITE will focus on the practical communication links that will assist in the management of the registries in the face of increasing cross border trade in a multi-language environment.We are deliberately using the generic term "entities" although what is being addressed here is primarily the identification of companies. The process of identification can be applied to any entity that is entered in a register. Apart from other business types, such as limited liability partnerships, credit unions or co-operatives, we could also be discussing company directors, auditors or disqualified persons. For ease of comprehension we refer in this document to companies only.

7 http://www.brreg.no/porvoo13/documents/reid_unique_company_identifier.pdf

consortium has just started its own numbering system called REID⁸ which proposes a syntax not very different to existing identification systems⁹.

Another EU funded project that has to be mentioned is the PEPPOL (Pan-European Public eProcurement On-Line) project¹⁰. PEPPOL is developing the prerequisites for cross-border governmental electronic procurement processes in order that any company (and in particular an SME) in the EU can communicate electronically with any European governmental institution for the entire procurement process. This comprehends a “Business Document Exchange Network” with service metadata interfaces/registries where senders, recipients and business entities in the registry are uniquely identified. It further comprehends the development of a “Virtual Company Dossier” (VCD) which shall enable suppliers to collect evidences from existing registries and to submit those evidences electronically to any public sector awarding entity in Europe. These evidences are proofs of compliance to a certain criterion usually supplied by an attestation or statement, e.g. an extract from a commercial register or a conformity assessment certificate stating the conformance to a specific quality assurance standard. (Please see chapter 6.2.8 “Presentment Of Conformity Assessment Certificates” concerning this topic.)

History Of Identification Schemes

It is obviously the ambition of the professional bodies to promote the usage of identification systems specific to their business sectors. Since its very beginning, the civil aviation has set up codes to make sure that cities in the world would be distinguished from homonyms in other countries or continents. ICAO¹¹, its international body, has proposed an identification based first of world regions¹², then on countries¹³, then on cities¹⁴ and finally on airports¹⁵. Later on, IATA, the syndicate of airlines has simplified the ICAO codification by suppressing the region code but as many countries have developed their infrastructure further – like Canada – they had no choice but to claim non-used letters (X, Y, Z). This is the reason why there is no obvious correspondence between a numbering system and what it identifies!

More recently the transport industry has announced its objective to provide a guideline for a Global Unique Identification of Transport Units known as the License Plate number. The method applied is based upon the International Standard ISO/IEC 15459 “Information Technology – Automatic Identification and Data Capture Techniques – Unique Identifier for Transport Unit Parts 1 & 2. E.g. the automotive industry uses transport labels according to ISO/IEC 15459 with unique partner identification. Odette’s transport label (OTL) and the Joint Automotive Industry Forum’s (JAIF – AIAG, JAMA/JAPIA, Odette) Global Transport Label recommendation both implement the ISO standard.

EUROMIND¹⁶, an initiative of the shipbuilding industry is working in the same direction to coordinate their activities between business partners.

8 The aim of the REID (Registered Entity Identifier) initiative is to establish a way in which entities in business registers can be identified by a number that is unique at the world level.

9 Country code + register id + ‘.’ + basic identification string + check sum

10 Please see <http://www.peppol.eu> for further information.

11 the International Civil Aviation Organization

12 for Western Europe France, Italy, Spain, Portugal

13 France becomes LF, Spain LE, etc.

14 Paris becomes LFP, Madrid LEM, etc.

15 Paris Orly is designated by LFPO, etc.

16 Develop a semantic webstack for integrated exchange of shipbuilding data between all parties and between all standards (or parts thereof).

Legal Background Of Identification Schemes

Both anti fraud activities and the current EU SEPA context are in favour of promoting unique identification of companies. This is being reinforced by the First Directive on Company Law which requires that “Member States shall stipulate that letters and order forms... shall state ...the information necessary to identify the register in which the file [...] is kept, together with the number of the company in that register”.

The same directive states, from January 1, 2007, that this information should also be on the company's web site. What is required is an external representation of the company number with additional information to identify the register within which the number is unique.

Since the 09/11 events, governments have realised the danger of new threats arising from tight relationships between organised crime and economy and how financial flows can effectively be used for money laundry purposes or dissimulate malevolent activities. On the other hand, the Internet and new communication means are more and more dematerialising activities therefore requiring that business relationships to be based on stable basics.

4.1.2 ISO/IEC 6523: Structure For The Identification Of Organizations And Organization Parts

General Syntax Of Identification Systems

The International Standard ISO/IEC 6523 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 32, *Data management services*. It consists of the following parts, under the general title *Information technology — Structure for the identification of organizations and organization parts*:

- *Part 1: Identification of organization identification schemes*
- *Part 2: Registration of organization identification schemes*

There is no common rule for setting up a company numbering system and the most recognised institutions propose private schemes. Standardisation schemes recommend starting with a country code - the most popular being ISO 3166-1 Alpha 2, to make sure that the registration place can be identified. This is not at all the case for private numbering systems, which prefer sequentially allocated digits ideally suited for powerful searches.

ISO then recommends a company's identification scheme and finally a check digit for verifying the overall coherence during routing or transfer procedures. As required by ISO/IEC 6523, an Organization Identification Scheme (OIS) is in charge of the unique identification of applicants. This registering body is referenced at ISO as an Issuing Organization (IO)¹⁷.

4.1.3 Overview Of Types Of Business Identification Schemes

The main challenge for a successful registration body relies not that much on its identification scheme but rather on the quality of the data it requests and verifies before the company gets its credentials. The evolution of stored data means that members would be the only ones entitled to ask for creation, deletion or modification of their entries. The service operator usually provides, in addition to the registration, various levels of services out of the data available within the repository¹⁸, which make his business profitable. Usually, repositories encompass functions not

¹⁷ ISO 6523 “A body that assumes responsibility for the administration of a specific organization identification scheme.” No further identification of an issuing authority or organization is required to create global uniqueness or identification. ISO maintains a list of IOs. Each IO is identified by an International Code Designator (ICD). The ICD is a number expressed as 0000 – 9999.

¹⁸ D&B's claims the following database activity: A new business opens every minute, A business files bankruptcy every 8 minutes, A business closes every 3 minutes, A suit, lien or judgment is filed against a company every 14 seconds, a chief executive office changes every minute, A company name changes every 2 minutes

only related to the allocation and publication of numbers e.g. search and documentation capabilities. Members are responsible for notifying changes to their data. However links with other industry repositories increase the quality of updates and the search capabilities.

Participants are entitled to search the database. However, there are access restrictions depending on the nature of stored data. Registered members may control which other entities can view their data (all or part of these).

Broadly, registration bodies can be divided in three models:

A centralised model¹⁹: The applicant goes to the registration authority to obtain an identification number, – directly or via an agent, who is in charge of filtering the application (accuracy, completeness of application).

A decentralised model²⁰: In this case, the applicant registers to a national authority affiliated to the main body. He might use an agent to ascertain the quality of the data provided for registration purposes

The “IBAN-like” model: this one does not require registration to a specific body. In this context, the norm allows applicants directly to issue account numbers based on open specifications (e.g. constructed around recognized domestic/local numbering schemes with the addition of e.g. a country code or a scheme issuer code.)

We will assess the various identification procedures, first the ISO driven – BIC/SWIFT, IBAN –, then the government originating and finally industry driven. We propose the following grid analysis: market situation of the identifier, its history and syntax rules, then finally, what additional capabilities it offers to its business customers.

TC 68 As The Standard Body Of The Financial Sector. History And Scope

The Technical Committee 68 (ISO/TC68) is the ISO structure entitled to develop standards and technical reports for financial services. This domain includes the following actors: depository institutions, like banks, non-depository institutions or finance companies, consumer and commercial lenders specializing in funds raising, both buy and sell side of the securities markets, private equity firms, mutual fund complexes, central banks, electronic clearing networks and other financial intermediaries, such as mortgage and insurance companies. ISO/TC 68 comprises three main subcommittees, SC2, SC4 and SC6:

- SC2: Security Management and General Banking Ops
- SC4: Securities and related Financial Instruments
- SC6: Retail Financial Services

Originally formed in 1948, ISO/TC 68 is growing in importance as new technologies, financial products and cross-border processes become complex and the demand for new practices and standardisation are more and more needed by all parties.

Most of the standards developed under the ISO/TC 68 umbrella have been adopted by member countries as their national standard. These have contributed achieving interoperability across boundaries, heterogeneous businesses sectors and reducing fraud. Furthermore, legal obstacles for the usage of electronic “financial transactions” have been overcome by the means of uniform

¹⁹ This is the typical D-U-N-S or Easy number model

²⁰ This is the typical GLN model

rules supported by IT systems. This yet allows seamless funds transfers for both consumers and business sectors.

Harmonization is becoming more stringent with the wide acceptance of the Euro among the Member States and outside the EU; this yet being increased with the implementation of the SEPA program. The recent demand for KYC and AML rules has leveraged further the implementation of finance standards, the final objective being the reduction of operating expenses for connecting business partners. In this context, the ISO/TC has prioritized its efforts to achieve the following goals:

- Wide implementation of “Straight Through Processing” or STP for business transactions
- Seamless financial transactions, data and infrastructure to avoid security gaps
- Migration of paper-based transactions to the benefit of end-to-end IT systems

Two Liaison Organizations are yet in charge of collecting, storing, disseminating and/or displaying data relevant to the standards they are responsible for:

- ANNA: Association of National Numbering Agencies (For the non-finance sector)
- SWIFT: Society for Worldwide Interbank Financial (For the finance sector)

Concerning the unique identification of companies, we propose to assess how the following ISO standards meet the demands of various business sectors for both providing search capabilities and securing business transactions between the companies.

- ISO 9362 BIC - Bank Identifier Code
- ISO 13616 IBAN - International Bank Account Number

Financial Identification Numbers

BIC: Bank Identifier Codes

Market Situation

BIC stands for Bank Identifier Code. These codes are used when transferring money between banks, particularly for international wire transfers and also for the exchange of other messages between banks. The codes can sometimes be found on account statements. Both BIC and IBAN (see below) are mandatory in the context of SEPA for wire transfers.

Recognition

The BIC format is often considered as the most acceptable format for neutral companies identifiers. The BIC is used globally and is in compliance with ISO15022 “Scheme for messages (Data Field Dictionary)”.

History

ISO 9362 (also known indifferently as **SWIFT-BIC**, **BIC code**, **SWIFT ID** or even **SWIFT** code inasmuch as the two identifiers are closely related) is a standard format of Bank Identifier Codes designed under the umbrella of the International Standard Organization (ISO). It is the unique identification code of a particular bank.

Syntax

The SWIFT syntax consists of 8 or 11 characters, made up of:

- 4 characters - bank code (only letters)
- 2 characters - ISO 3166-1 alpha-2 country code (only letters)
- 2 characters - location code (letters and digits) (if the second character is '1', then it denotes a passive participant in the SWIFT network)
- 3 characters - branch code, optional ('XXX' for primary office) (letters and digits). Where an 8-digit code is given, it may be assumed that it refers to the primary office.

Additional Services

SWIFT Standards, a division of The Society for Worldwide Interbank Financial Telecommunication (SWIFT), handles the registration of these codes. For this reason, Bank Identifier Codes (BICs) are often called SWIFT addresses or codes.

There are over 7,500 "live" codes (for partners actively connected to the BIC network) and an estimated 10,000 additional BIC codes which can be used for manual transactions.

Additionally SWIFT has issued BICs to entities that need to be identified in Swift messages but are not Swift members. These are called BIC1s because a "1" is always placed in the eighth position of a BIC1 to distinguish it from a BIC.

IBAN: International Bank Account Number

Market Situation

Standing for International Bank Account Number, IBAN is a finance numbering system designed to identify bank accounts internationally. Originally adopted by the European Committee for Banking Standards, it was later adopted as ISO 13616:1997 and now as ISO 13616:2007. The official IBAN registrar under ISO 13616:2003 is SWIFT. An IBAN is always used in conjunction with a SWIFT/Bank Identifier Code (BIC). Most banks in Europe (excluding those in the CIS) provide an IBAN identifier for their accounts as well as nationally recognised identifiers. In addition, Israel, Tunisia, Mauritius, Turkey and Saudi Arabia also provide IBAN format account identifiers.

The ECBS expects that adoption may take up to ten years, so it remains necessary to use the current ISO 9362 Bank Identifier Code system (BIC or SWIFT code) in conjunction with the BBAN or IBAN.

Banks in the British dependencies (except Gibraltar and the Crown Dependencies) do not use the IBAN format, but this may be due to internal banking regulatory issues. Some banks outside of Europe may still not recognize IBAN, though as time passes this is expected to diminish.

Banks in the United States do not provide IBAN format account numbers. Any adoption of the IBAN standard by U.S. banks would likely be initiated by ANSI ASC X9, the U.S. financial services standards development organization but to date it has not done so. Hence payments to U.S. bank accounts from outside the U.S. are prone to errors of routing. Additionally US banks use the Universal Payment Identification Code (UPIC). It is an identifier for a bank account in the United States allowing the account owner to receive electronic credit payments without revealing the account number or risking unauthorized direct debits from the account.

The Canadian banking system has adopted IBAN for international transfers, but to date it is only a marginal part of consumer international transfers because NAFTA centric money transfer entities manage most money transfers under \$10 000 in the NAFTA area.

Australia and New Zealand have adopted IBAN for international money transfers.

Recognition

IBAN was originally developed to facilitate payments within the European Union but the format is flexible enough to be applied globally. IBAN imposes a flexible but regular format and validation data to avoid errors. It is a standard way of uniquely identifying an account for the purpose of improving the efficiency and speed of inter member-state EU payments. It is not a new bank account number but rather a way of representing these in an internationally recognised standard format. Currently all the SEPA countries have adopted the IBAN format for banks accounts identification. Since January first 2007, wire transfers are processed based on IBAN and BIC codes for all EU, including those outside of the Euro zone.

History

Ever since from Dec 2001, EU Regulation 2560/2001 requires banks to provide the IBAN and their SWIFT/BIC to their account holders in EU countries. IBAN was implemented to carry on the routing procedures so that a payment can be issued from one bank to another, irrespective of the country, the check digit confirming that the transaction would be completed. IBAN is not an identification scheme but rather a means to confirm that a transaction will complete.

Syntax

Customers, especially individuals and SMEs, are frequently confused by differing national standards for bank account numbers. IBAN imposes a flexible but regular format for account identification and contains validation information to avoid errors of transcription.

The IBAN's primary purpose is therefore to facilitate routing and avoid errors.

The length of IBAN can go up to 28 digits starting from 2 letter country code, specific to each country. It is made up of the following elements all stuffed to form a single one length format:

- Two-letter country code (CC) ISO 3166-1 alpha-2 country code
- Two-number check digit (CD) for the entire IBAN account number (from 00 to 96).
- Basic Bank Account Number (BBAN), no more than 30 characters long, comprising Institution Identification (IID) and Bank Account Number (BAN)

The length of IBANs is determined by each country, but is standard within the country.

Additional Services

The significant advantage of using IBAN is that the money sender will be charged at the rate of domestic transfers²¹, if the sender initiates the payment to any EU country within an EU zone under the following conditions:

- The Payment is made in EUR
- The total amount is less than EUR 12,500
- IBAN account number is specified along with BIC/SWIFT code of institution.

The routing of payments internationally requires the payer to inform the sending bank of the location of the receiving account (bank name, branch address) as well the account number of the

²¹ Made possible by the elimination of routing errors achieved using IBAN

destination account. The location of the receiving account is often identifiable from various routing codes which are often specific to the national payment system, and therefore are more readily machine processed than are names and addresses.

National routing codes and account numbers often (but by no means universally) contain check digits which are used nationally to help detect transcription and routing errors before payments are sent. However because national systems vary there was no common format for giving routing information that could be applied internationally.

Prior to IBAN therefore, it was impractical for banks to validate such routing information prior to the sending of payments. Routing errors were therefore frequent causing payments to be delayed and often created costs to the sending and receiving banks and often to intermediate routing banks also.

The standard IBAN is intended to carry all the routing information needed to get a payment from one bank to another. IBAN contains check digits which can be validated in any country according to a single standard procedure. The IBAN contains all the key bank account details and where used has reduced transnational money transfer errors to under 0.1% of total payment.

In this way, the validity of a routing destination can be validated by the sending bank (or its customer) from a single string of data which contains all the necessary routing data to get money into the destination account and routing errors in international (or cross-border) payments are therefore virtually eliminated. The IBAN system has adequate security measures such that publication the number poses no problem to the account holders.

IBEI: International Business Entity Identifiers

Market Situation

The usage of the **International Business Entity Identifier (IBEI)**, primarily called **LEI** or Legal Entity Identifier) has been imposed by the ever-increasing compliance requirements regarding the unambiguous identification of business entities in particular with respect to inter member-state business activities. Obligations imposed by KYC (know your client) and AML (anti-money laundering) procedures, MiFID, Basel II and G30 recommendations led the International Organization for Standardization (ISO) to develop the IBEI. The IBEI is a standardized code, which is allocated to legally independent entities (Legal Entities). Individual persons do not qualify for IBEI allocation. In a first step, the IBEI is provided for the financial industry, i.e., for all entities playing a role in the lifecycle of a financial instrument. The IBEI has been developed by the ISO working group ISO/TC 68/SC 4/WG 8.

IBEI is another identification scheme specifically dedicated to financial activities, but based on an international standard, rather than on proprietary information. Its role is to describe a BE (Business Entity), or wholesale financial market participants such as broker dealers, clearers, custodians, investment managers (including mutual fund managers, insurance fund managers and funds), banks (including central banks, investment banks, universal banks, banks and private banks), CSDs (national and international), exchanges (including ECNs, ATSS, MTFs), industry utilities (including outsourcers, ASP services, administration service providers), data providers (essentially company information and market data providers), regulators (including self regulating organizations and commissioners), and institutions which are funds or manage funds on behalf of others (including pension and insurance funds and trusts), charities, local and national governments, supra-national bodies and corporate treasuries, but not individuals. The BE may or may not be a legal entity.

Also, once such a standard gains international consensus and receives the recognition that comes with ISO approval, it will become a major tool for electronic messaging applications as it provides powerful building blocks for Straight Through Processing process.

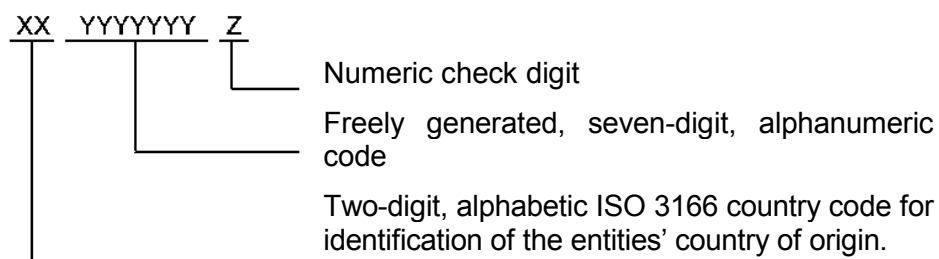
History

IBEI - which stands for the Identification of Business Entities - has been promoted by the SWIFT community since the 1990s as a potential solution to extend the usage of the BIC syntax to various institutions, not only originating from the financial sector. The proposed syntax was mainly designed for two purposes, on one side, compliance with KYC and, AML rules, on the other side, facilitate STP, or Straight Through Processing between business partners.

Syntax

IBEI is based on a 8 character BIC format. It is used to identify a unique regulated entity or its equivalent for non-regulated entities. It was designed as a 'final solution' to the problem of linking to and identifying the underlying fund for a financial transaction.

The originating idea is that the relationship between banks/branches is quite similar to the relationship between entities and funds. There is no hierarchy within the structure of the IBEI. The links between the different entities identified with an IBEI will be left for in house database or vendors' products. This can be summarised as follows:



The IBEI is allocated through central agencies for all entities, irrespective of an entity's own securities issue or the inclusion of own issues in organized or regulated markets.

Non Financial Identification Numbers

GLN: GS1 Global Location Number

Market Situation

GLN is derived from the international GS1 standard used to identify products in the context of supply chain and logistics activities. GS1 was formerly known as EAN international, a barcoding standard which is a superset of the original 12-digit Universal Product Code (UPC) system developed in North America. The **EAN-13** barcodes are used worldwide for marking retail goods.

GLN is a numbering system applied to logistics to locate companies and their different premises. Global locations numbers are reference keys to computer files where information about the company or location can be found. The GLNs replace the names and addresses of locations and are particularly useful when automating processes; they allow computers to route information to the correct destination with no manual involvement.

The GLN (Global Location Number) provides a standard means to identify legal entities, trading parties and locations to support the requirements of electronic commerce. The GLN is designed to improve the efficiency of integrated logistics while contributing added value to the partners involved, as well as to customers. Examples of parties and locations that can be identified with GLNs are:

- *Legal entities/Trading Partners* – e.g., buyers, sellers, whole companies, subsidiaries or divisions such as suppliers, customers, financial services companies, freight forwarders, etc.
- *Functional entities* - e.g., a purchasing department within a legal entity, an accounting department, a returns department, a nursing station, a ward, a customer number within a legal entity, etc.
- *Physical locations* - e.g., a particular room in a building, warehouse, warehouse gate, loading dock, delivery point, cabinet, cabinet shelf housing circuit boards, room within a building, hospital wing, etc.

Recognition

GLN provides solutions both for the identification of physical locations and their corresponding entities. GLN is used in bar coding, EDI and RFID applications.

History

GLN benefits of the wide potential of the **GS1 System**, e.g. a series of standards designed to improve supply chain management. It is composed of four key product areas: Barcodes (used to automatically identify things), eCom (electronic business messaging allowing automatic electronic transmission of data), GDSN (Global Data Synchronisation Network which allows partners to have consistent item data in their systems at the same time) and EPCglobal (which uses RFID technology to immediately track an item).

It has headquarters in Brussels (Belgium) and Lawrenceville, New Jersey (USA). There are also Member Organization offices in over 100 countries globally.

Syntax

The GLN is simply a 13-digit number used to uniquely identify any legal entity, functional entity, or physical location. Its basic components are:

- A GS1 Company Prefix
- A Location Reference
- A Check Digit

GS1 Company Prefix →	← Location reference	Check Digit
N1 N2 N3 N4 N5 N6 N7 N8 N9 N10 N11 N12		N13

GS1 Company Prefix - The globally unique number assigned to a company by a GS1 Member Organization. GS1 Company Prefixes are assigned to companies in varying lengths.

Location Reference – The number assigned by the holder of the GS1 Company Prefix to uniquely identify a location within the company. The Location Reference varies in length as a function of the GS1 Company Prefix length. The combined length of the GS1 Company Prefix and Location Reference is always 12-digits.

Check Digit – A calculated one-digit number used to ensure data integrity. Information on how this digit is calculated is provided at www.gs1us.org/checkdig.

GLNs can be encoded in 128 symbols and physically marked onto the items (barcoding).

Additional Services

By definition, GLN may be complemented by extension components to specify a physical location up to any required granularity. This can be the case for subsidiaries as well as any storage facility, like a shelf in a store as might be required by logistics needs. All locations, irrespective of the country, are identified in a unique manner.

Odette Code

Market Situation

Odette creates standards for e-business communications, engineering data exchange and logistics management which link over 4000 companies in the European automotive industry with each other and with their global trading partners.

A specific focus of Odette's activities since its foundation 25 years ago has been the identification of business partners involved in the exchange of 'mission critical' data via the Odette File Transfer Protocol (OFTP).

The identification scheme developed by Odette is now the predominant identification scheme for data exchange stations in the European automotive industry and is also used in several other industries such as transport, finance and retail.

This identification scheme is also used by many companies in the European automotive industry to identify partners and third parties in EDI messages.

Recently the Odette scheme has been further developed to meet the requirements of auto identification applications in the automotive supply chain such as parts marking, asset identification and transport unit labelling.

The Odette web-based application known as OSCAR (Odette System of Coding and Registration) allows companies to register their entity details and obtain entity codes on-line. Codes can be assigned to legal and non-legal business entities and the system is able to reflect hierarchical company structures.

The codes and the related data sets can be queried to the full extent by registered OSCAR users and to a more limited extent by the general public.

Syntax

The Odette (OSCAR) Code is a 4 Character Code assigned to main business entities, which can be extended by a 2 character extension for sub-entities.

For B2B applications such as OFTP and EDI, the OSCAR code is used in accordance with ISO/IEC 6523. A typical code for EDI applications could look like this:

0	1	7	7	A	B	0	3	0	2
---	---	---	---	---	---	---	---	---	---

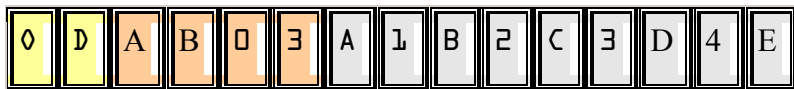
- 0177 - The ISO ICD identifies the assigning organization. Odette is registered at ISO as an issuing organization with the ICD 0177
- AB01 – Main business entity code
- 02 – sub business entity code.

For data transmission as a data exchange station identifier the OSCAR code follows the historical 25 character specification of the OFTP protocol:

0	0	1	7	7	0	0	0	0	0	0	0	0	0	0	0	X	0	0	8	0	0	0	0	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

- O: Qualifies the ID as OFTP ID
- 0177 : The ISO ICD
- 0000000000X008: The ID assigned by OSCAR, with leading zeros to fill the format of the OFTP identifier (alphanumeric, 14 characters).
- 000000 (Sub address): The internal sub-address or system name (e.g. "PLUTO1"). If no sub address is necessary, 6 zeros can be used.

For Auto ID applications such as Transport Unit Labelling, Asset Identification and Parts Marking, the OSCAR code is used in accordance with ISO/IEC 15459. A typical code for Transport Unit Labelling could look like this:



Government Numbering Systems

Many EU countries are operating their national numbering system. If we consider the case of France, the SIRET is composed of 14 digits broken down in two parts. The first one is called the SIREN number, the latter, usually called NIC (Internal Classification Number) is made of a sequential number (4 digits) different for each office location and is terminated by a check digit. The SIREN number is the only means to communicate with the French government for admin issues. It is currently generated by INSEE²² and the company submits its application to the national registry of commerce²³; The APE²⁴ or NAF²⁵ code is the national version of the EU NACE²⁶ code. Each country has its own process; certain utilize industry identification schemes, others rely on government registration services²⁷.

The EU has recently supported the initiative of a centralised access that would connect to the national systems. Under the banner of the EBR²⁸ (European Business Register), the information is retrieved directly from the respective country's official company register. The registers are updated regularly by national partners.

EBR does not at all provide a unique identifier but rather allows making queries on national databases. There are different kinds of reports available depending on the country's registration process and the company's data. EBR always provides minimum corporate profiles like the company's name, registration number, address, country of registration, date of registration, registration authority, legal form, current status, type of business activities, share capital, date of the latest annual account. The information is brought from the source. The Company Profile is available from all the participating countries. Some national registers also provide information on the board of directors, management owners/shareholders and annual accounts.

²² National body for statistics and economical studies

²³ RCS , Registre du Commerce et des Sociétés

²⁴ APE : Activité Principale de l'Entreprise

²⁵ NAF Nomenclature des Activités Françaises

²⁶ NACE Nomenclature d'Activités Européenne: 4 digits + 1 country digit

²⁷ E.g. Registre du Commerce et des Sociétés

²⁸ Company registry or EBR at the EU level <http://www.ebr.org/>

VAT Registration Number

History

Under the new VAT (Value Added Tax) system, intra-Community supplies of goods are exempt from VAT in the Member State of despatch when they are made to a taxable person in another Member State who will account for the VAT on arrival. Therefore any taxable person making such supplies must be able to check quickly and easily that their customers in another Member State are taxable persons and do hold a valid VAT identification number.

Market Situation

For that purpose, *inter alia*, each tax administration maintains an electronic database containing the VAT registration data of its traders. Such information includes the VAT identification number, the date of issue, the trader's name, the trader's address and, where applicable, the date of cessation of validity of a VAT number.

A computerised VAT Information Exchange System (V.I.E.S.) was set up by the EU to allow for the flow of the data held across the internal frontiers which:

- Enables companies to obtain rapidly confirmation of the VAT numbers of their trading partners
- Enables VAT administrations to monitor and control the flow of intra-Community trade to detect all kinds of irregularities

The unit responsible for the control of intra-Community trade in each Member State, the Central Liaison Office (CLO), has a direct access through VIES to the VAT registration database of the other Member States. Even though the VIES offers a VAT control scheme, it does not provide sophisticated intra-EU query capabilities as it is the case for the financial services mentioned hereafter.

Syntax

A VAT registration number is an alphanumeric sequence which consists of up to 15 characters without space. The first two letters indicate the respective member state, for example DE for Germany. All vendors who are entitled to deduct VAT can receive a VAT registration number from their local tax authority. **e.g. GB12345678**

The VAT number is given by national tax authorities and is based on algorithms used by the Member States; it is unique for a company and does not change over its life. It can be consulted via databases for all companies registered in the EU, as well as through a single point of contact made available by the EU Commission.

This number shall be visible on all bills issued by a company irrespective of the location its activities are performed. Furthermore, it is shown on all VAT forms. The aim of this identifier is to warrant the exchanges between companies across the European Union.

Industry Driven Numbering Systems

Besides the ambitious initiatives carried on under the banner of the International Standardisation Organization, the financial sector is additionally operating its own identification systems. The two approaches are more complementary than really competitors. On one side, ISO sets up the rules for implementing IT measures and facilitating fund transfers between business partners; on the other side, financial institutions are providing powerful query systems and international recognition to their customers members.

D-U-N-S Number

Market Situation

D-U-N-S, which stands for D-U-N-S = Data Universal Numbering System, is certainly the most popular registration system issued from the financial sector. Its objective is to define business entities as a whole by integrating their various corporate structures together. It defines corporate firms starting from headquarters and integrating subsidiaries and foreign branches. A specific DUNS number is assigned to each business location in the D&B database having a unique, separate, and distinct operation to businesses for the purpose of identifying them. A DUNS Number remains with the company location to which it has been assigned even if it closes or goes out-of-business.

Recognition

Worldwide accepted, D-U-N-S accounts for more than 140 million corporate entities. Due to its international recognition, it is favoured by major industry and trade associations across the world, including governmental bodies like the UN, the U.S. Federal Government, and the European Commission. D-U-N-S registration requires a quality compliance procedure called DUNSRight TM. It is recognised as a quality award which guaranties the reliability of the worldwide D&B network.

History

D-U-N-S is a service of the financial Dun & Bradstreet firm created in 1962. Even though it is distributed freely²⁹, it provides firms with a strong visibility on the market place as it is mandatory to enter business practices with certain major firms. It is a source of information for checking the creditworthiness and stability of companies. Its nine-digit structure allows to present firms structures on a national and international level. D-U-N-S has greatly increased over the last five years due to the growing registration of companies from emerging countries aiming for international recognition. The DUNS number has replaced back in 2005 a former coding system known as ACASS (**Architect-Engineer Contract Administration Support System**).

Syntax and Directory Structure

D-U-N-S proposes a quite simplified syntax based on the unique combination of NNNNNNNNNN, where each N represents a number from 0 through 9; hyphens and spaces are not allowed. It is shown in the form DUNS NNNNNNNNNN without any possibility to identify the country and the business sector of trading parties. The number is randomly issued and the digits apparently have no significance as to their issuance. Until approximately December 2006, the DUNS number contained a Mod 10 check digit to support error detection. The check digit was discontinued to increase the inventory of DUNS numbers available for assignment by 800 million. A DUNS number is sometimes formatted with embedded dashes to ensure its readability.

The objective of the D-U-N-S numbering system is to provide a powerful query mechanism based on the following data:

- Name of the organization
- Organization address
- Name of the CEO/organization owner
- Legal structure of the organization (corporation, partnership, proprietorship)

²⁹ When obtaining a DUNS number online, the wait can be as long as 30 days. When requesting a DUNS number by phone and paying an investigation fee, it is issued immediately.

- Year when the organization started
- Primary type of business
- Total number of employees (full and part time)

The DUNS Number also "unlocks" a wealth of value-added data associated with that entity, including the business name, physical and mailing addresses, tradestyles ("doing business as"), principal names, financial, payment experiences, industry classifications (SICs and NAICS), socio-economic status, government data and more. It also links members of corporate family trees worldwide.

EasyNumber

Market Situation

EasyNumber is an identification initiative launched to meet the demand of internationally operating companies irrespective of their business activity. Rather than a sector numbering scheme, it is an open initiative aiming to provide a universal identifier for searching and uniquely identifying companies throughout the world. Same as the D-U-N-S, its objective is to provide for a neutral approach to facilitate opportunities between internationally operating businesses.

Recognition

This repository maintains a high quality up-to-date file of global businesses, which is the basis for providing seamless online access to a global network of international firms. The global network of Partners maintains value-added business information directly linked via their EasyNumber. To date, EasyNumber registers more than 50 million of EU and US companies in its database.

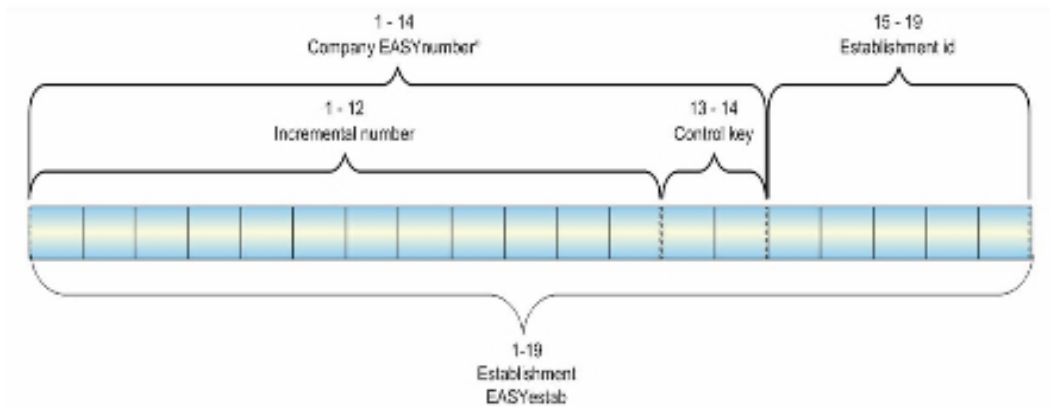
History

Creditreform and Coface, respectively No. 1 and No. 2 in the European Credit Management services sector, provide the registration scheme.

Syntax

Same as for the D-U-N-S, the EasyNumber syntax consists of numbers sequentially allocated with no direct link to country of origin or business sector. More specifically, it contains 19 digits:

- The 14 first digits are the Company's Number
 - 12 incremental digits
 - The next 2 digits are a control key
- The last 5 digits identify the establishment (branch) of the company.



1st Establishment (head office) = 000005011155 22 00001

2nd Establishment (branch) = 000005011155 22 00002

Additional Services

The EasyNumber system provides the following features:

- Powerful searching to uniquely identify companies anywhere in the world
- Simplified access to a comprehensive and reliable worldwide company database
- Allocation of any business worldwide with a single, unique and universal ID, complementary to national ID numbers
- Permanent maintenance of worldwide company's identification information
- A web-based toolkit to easily integrate services into proprietary software applications
- The basis for accessing value-added business information from a growing worldwide network of content providers who maintain identifiable data
- The basis for depicting global company ownership structures

In addition to the numbering scheme, EasyNumber provides a comprehensive repository consisting of up to 9 indexed identification data elements per business or establishment

- Company name
- Address
- Local identifier(s)
- Telephone
- Legal form
- Establishment detail (Head office or branch)
- Company status (active / inactive)
- Trade names
- Activity code

CREFO Number**Market Situation**

Crefo Number is another sector application aiming to facilitate the assessment of creditworthiness between business partners based on an unequivocal identification of the parties. This applies both to corporate firms and individual consumers by providing reliable data about the registered office of a company or the place of residence of a private individual.

Crefo offers a complete automation of the purchase order assessment (identification and solvency rating) for companies that propose their products and services via electronic marketplaces. The software identifies and evaluates the creditworthiness of B2B customers in form of a traffic light function. The application of e-crefo is particularly effective in bulk business with low order values or rather credit amounts with high costs for credit checks. E.g. Internet service providers and mail order business, operators of electronic marketplaces or teleshops.

History

Most of the companies in Germany and Austria have their ten-digit number from Creditreform - the so called "Crefo number". It is unique and permanently updated with information by more than 1000 researchers and data administrators. To date, more than 3.6 million companies are registered in the database.

Additional Services

A fully automated process allows a subsequent enrichment by adding creditworthiness information. The complex procedure is based on various query functions. Various search tools are provided such as search by the means of synonyms, and fuzzy research allowing the possibility of getting more and more precise results. Searches facilities are reserved to registered members.

4.2. Questionnaire For Issuers Of Unique Identifiers

ISO/IEC standard 6523 "Structure for the identification of organizations and organization parts" covers most existing organization identification schemes. However, Unique Identification of business entities is one side of the problem. The reverse side is Verification of the related organization.

In order to establish what types of identification schemes are actually used, it was decided to publish an on-line questionnaire to gather information to complement the initial desk study performed. The questionnaire targeted the issuers of unique identifiers and tried to gather information reflecting the procedures used for identifying entities, structures of identification and legal and IPR issues involved.

Initially there was a 40-question "long" questionnaire designed, but later on it was decided to limit it down to the most important 13 questions, which were then put on-line. The questionnaire was made available only on-line for a period of one month. Invitations were sent to fill out the questionnaire to all members of the working group, as well as to the European Business Register (EBR)³⁰ members. EBR is a network of business registers kept by the registration authorities in most of the European countries.

The complete questionnaire, together with the detailed description of the replies, can be found in the Appendix of this document. Here we present a summary of the results.

³⁰ <http://www.ebr.org>

There was a total of 21 answers received (17 fully completed and 4 incomplete). The analysis was performed on the 17 fully completed questionnaires that were received.

The first question concerned the purpose of registration: was it meant to unambiguously identify an organization – or not? Out of the 17 answers, received 14 were positive and 3 negative.

The second question was on the provision of the identification scheme to identify constituting parts (products, units etc.) within the organization. 10 of the 14 previous positive replies were also positive.

Out of the 11 schemes that allowed for identification of constituting parts within the organization, 3 allowed for this identification to be done by the organization itself and in another 7 cases the identification of the constituting parts within the organization was done by the assigning organization.

The Identification schemes in use follow different layouts (various alphanumerical structures) and only in four cases are they dependent on an external register. In most of the cases the registration procedures are publicly available through the Issuing Organization's website.

The allocation/registration procedure for the allocation of an identifier differs from issuing organization to issuing organization. The necessary documents are either provided by the registrant or assumed by an existing membership in an acknowledged registry.

In the majority of the cases (15/17) identifiers that have already been used are not reassigned after the deletion of entries.

The application areas for which the registration data is put in use have to do with basic business entity identification in various areas. The most common are:

- State use
 - Tax authority
 - Statistics
 - Pension funds
 - Health information systems
- Bank use
- Commercial use
 - Trade partners identification/information
 - Audiovisual content
 - RFID
 - Libraries

In the majority of the cases the content of the register is publicly available from the respective organization website.

As for meta-identification schemes used or recommended for the meta-identification of the identifier-scheme, there is mixed feeling. Many organizations do not use any meta-identification scheme or see no need for it. For the ones seeing usage in this area the answers were using the OID based on ISO/IEC 6523 or ISO/IEC 15459, or the Company name and number, or an OID.

In more than half of the replies, the identifier has a legal effect, usually having to do with unique identification within the public sector, tax authorities, social security and banking or with the identifier having to be provided with all company documents related to the Register of Commerce and Trade. This identifier is available in all databases related with these topics and is very widely spread for both online and offline applications. The company number has to appear on all business stationery. Incorporation also allows a company to exercise its business activities and borrow money etc.

In most cases, the company does not own the copyright to the identifier itself, which is held by the Issuing Organization. Finally, the Issuing Organization usually does not pose any restrictions on the usage of the identifier.

5. Part 2: Inventory Of Applications And Associated Requirements

5.1. List Of Application Areas

In order to assess application areas with regards to the scope of this CWA the following applies: The specific usage of unique identifiers and combinations thereof has to be considered. The focus is on open systems and user groups. In all application areas, identification schemes are the basis for the improvement of processes by reducing the overhead of manual workflows and ideally the full automation of these processes. Often the legal certainty of a transaction is enhanced or enabled by a unique identification scheme as well, e.g. by applying a VAT- or commercial register number.

As a consequence, application areas can be listed in a matrix versus main usage/focus of unique identifiers, type of interaction, type of registration (public/private) and the structure of an identification scheme (i.e. if the organization part is useful or not).

Table 1 - Assessment of Application Areas With Regards To Identification Schemes

Attributes Application area	Main focus of using unique identifiers	B 2 B	B 2 C	B 2 G	C 2 G	Type of registration, i.e. registrar		Organizational part in identification scheme useful
		B	C	G	G	public	private	
eCommerce/ eBusiness	Building of trust and STP, Straight Through Processing	x	x	x		x	x	x
eProcurement	STP, Straight Through Processing	x		x		x	x	x
Supply chain/logistics processes	Parts marking (manufacturer identification), shipping labels (sender identification), ownership of (reusable) transport items	x		x			x	x
eInvoicing (concerning business requirements)	STP, Straight Through Processing	x	x	x		x	x	

<div>Attributes</div> <div>Application area</div>	Main focus of using unique identifiers	B 2 B	B 2 C	B 2 G	C 2 G	Type of registration, i.e. registrar		Organizational part in identification scheme useful
						public	private	
VAT valid eInvoicing (concerning taxation requirements): at least one partner is liable to VAT	Effectual against VAT administration	x		x		x		
VAT declaration by VAT liable subject	Validity, ease of use			x		x		
ePayment by companies or consumers	Ease of use	x	x	x	x	x	x	
Banking procedures	KYC ("Know Your Customer") and AML (Anti Money Laundering) principle	x	x	x		x	x	
Credit procedures: interaction between Bank and credit user	Building of trust	x	x			x	x	
Social security, employment procedures	Ease of use		x	x	x	x		
Registered e-mail	Ease of use, probative force w.r.t. sender/recipient	x	x	x	x	x	x	x
Document management in general	Probative force w.r.t. auditing;	x	x	x	x	x	x	x
Archiving	Easy retrieval	x	x	x	x		x	x
Accreditation bodies accrediting conformity of assessment bodies	Professional checking of conformance	x		x		x		
Relying on certificates issued by conformity assessment bodies	Building of trust	x	x	x		x	x	x

5.2. Meta-Identification Schemes

5.2.1 Introduction

Interoperability between different identification schemes can only be achieved by working with meta-identification, i.e. a system that forms an umbrella over existing systems by assigning identifiers to identification schemes, an approach which guarantees both independence and flexibility (as described in chapter 1 “Scope”) of the Issuing Organizations and their participants or customers. This chapter gives first an overview over the most relevant meta-identification schemes for the purpose of unique organizations’ identification in open environments. It then discusses their applicability as global meta-identification systems and finally proposes recommendations for further implementation. Please note that persistence is an important feature of meta-identification schemes.

5.2.2 Inventory

The following meta-identification schemes have been identified as meeting the (governmental and business) requirements in terms of persistence, standardisation capabilities, proper documentation and applicability. In addition, these schemes are relevant as they are referenced in other (industry) standards and/or are used in practical implementations.

ICD According To ISO/IEC 6523-2

ISO/IEC 6523-2 “Structure for the identification of organizations and organization parts — Part 2: Registration of organization identification schemes” defines a meta-identifier scheme, the International Code Designator (ICD). ICD values are numerical values of up to four digits. It also defines registration procedures for the allocation of an ICD value to an identifier scheme and designates the British Standards Institute (BSI) as the registration authority. As ISO/IEC 6523 is specifically designed for “the identification of organizations and organization parts ” ICD values are often used within the scope of this document.

Example:

0088 is the ICD value assigned to the Global Location Number (GLN) scheme of GS1.

OID According To ISO/IEC 9834-1

ISO/IEC 9834-1 “General procedures and top arcs of the ASN.1 Object Identifier tree” describes procedures applicable to the registration of objects. Furthermore it specifies the hierarchical structure of the registration naming-domain and provides guidelines for the establishment and operation of Registration Authorities. Finally, it establishes the Object Identifier (OID) hierarchy as a tree whose nodes are numerical values. Despite their origin in the OSI world, OIDs can be used in any context. The OID tree is based upon distributed registration. This provides a high flexibility as an advantage, but involves that an identification scheme might be registered under more than one arc and that not all OID’s are verifiable in a public directory³¹.

The OID scheme comprehends other meta-identification schemes as well. Under the arc³² *{iso(1) identified-organization (3)}* ICD values as discussed above and specific (numeric) identifiers can be included in the OID scheme.

³¹ The best directory available is the OID repository at <http://www.oid-info.com> where any user can submit information about an OID he owns or has knowledge of. This OID repository contains all OID’s defined in all ITU-T Recommendations, all IETF RFCs and some ISO International Standards.

³² A branch of the of the OID tree is called “arc”

Example In the OID 2.16.56, the leading “2” designates a joint registration scheme of ISO and ITU. The following “16” represents the country specific registration scheme and “56” designates the country Belgium. Under this OID, national Belgian identification schemes can be registered.

URN According To RFC 2141 And 2396

RFC 2141 “URN Syntax” and RFC 2396 “Uniform Resource Identifiers (URI): Generic Syntax” specify the characteristics of the Uniform Resource Name (URN) and set the scene for the suitable implementation.

Within this scheme, the node “URN” is always the root node. RFC 3406 “URN Namespace Definition Mechanisms” explains how to establish nodes - or namespaces as they are called within this terminology - beneath the root node. It also specifies the registration procedure for namespaces at the Internet Assigned Numbers Authority (IANA) which acts as a Registration Authority. See <http://www.iana.org/assignments/urn-namespaces/> for a list of formally registered formal URN namespaces. Similar to the OID scheme, the registration below these registered namespaces is distributed and not all registered URN’s can be verified in a public directory.

The URN-scheme comprehends other meta-identification schemes as well. The registered formal namespace “OID” (as specified in RFC 3061) provides the possibility to include OID’s as described above.

Please note the fact that the root node “urn” is always declared, i.e. that every URN starts with “urn:..” makes the URN scheme highly self-descriptive.

Example:

The “Organization for the Advancement of Structured Information Standards (OASIS)” has registered the namespace “oasis” within the URN-scheme. Under “urn:oasis:” namespaces for including organization identification schemes have been specified, such as e.g.

urn:oasis:names:tc:ebxml-cppa:partyid-type:iso6523:0106.

ISO 7372

ISO 7372 “Trade data interchange - Trade data elements directory” lists standard data elements intended to facilitate open interchange of data in international trade. The data element 3055 in combination with the data element 1131 can be used as meta-identification of unique business identifiers.

Example:

1131	3055	COMMENT
1	16	The coded data element value used in association with 1131/3055 is one maintained by Dun and Bradstreet (3055="16"), in the DUNS list of enterprise numbers (1131="1").

5.2.3 Interoperability

Interoperability in eBusiness and eGovernment does not only concern agreed technical formats of documents and protocols among (trading) parties (syntactic interoperability), common vocabularies and ontologies for business processes, but rather also an agreement on the identifiers and especially what meta-identifiers will be used.

This implies a consensus on the trustworthiness of the applied identification schemes and the registers, which hold the designated information. In order to create a maximum benefit out of this

information, the lookup of identifiers and meta-identifiers in registers needs a common basis in order to work globally. The same holds true for the mapping of an entity's different identifiers.

There must be well-described, economic and accepted ways to select what data shall be designated by a meta-identification scheme, i.e. to detect which identification scheme is meta-identified. In addition, a (meta-) identification scheme should integrate business relevant information in a straightforward manner. Therefore, the registration to a meta-identification scheme requires a specific quality of information gathered.

5.2.4 Mapping

Different identifiers are currently used to identify and authenticate the same organization across various contexts. However, one single business transaction usually covers more than one context: E.g. an Order-To-Cash Cycle might involve the following data: first, an identifier for business rating of the prospective customer, another one for supply chain issues, then a VAT-number assigned by a public administration and finally an account number for payment.

Therefore, lookup of a specific identifier with another identifier as input as well as proofing that two or more identifiers belong to the same organization for audit reasons needs mapping mechanisms.

Possible ways to implement mapping are:

- Designated databases:
Information in a database about a business entity specified by an identifier provides other identifiers pointing to information concerning the same identified entity.
Example:
The Australian Taxation Office³³ provides a public interface to a database that can be queried via the Australian Company Number (ACN). The retrieved information contains the Australian Business Number (ABN) of this company.
- Self-declaration:
An organization or one of its entities can declare different identifiers that designate this organization or entity for different purposes.
Example:
A typical example of self-declaration is that of a company which publishes its Commercial Register Number, the VAT-number and/or its IBAN on its corporate website.

The presentation of a mapping – depending of the possibilities and requirements – may be performed in different (non-exclusive) means.

- Different identifiers can be included in documents stating that the entity is designated by several referencing identifiers. These documents may be:
 - o Machine-readable:
No *dedicated* standard for mapping of unique identifiers exists. However, the ebXML Collaboration Protocol Profile and Agreement (CPPA) Specification allows the mapping of unique business identifiers. This is achieved by including more than one “PartyID” elements in a “PartyInfo” element.
In addition, the Resource Description Framework (RDF) is designed to express entity-relationships. Therefore, RDF can also be used for the mapping of identifiers.
 - o Human-Readable:
The usual way to present unique business identifiers in electronic human readable documents, especially when it comes to (official) organization identifiers are the HTML- and PDF-format.

33 See <http://www.abr.business.gov.au/>

- The different identifiers may also be embedded within a Uniform Resource Identifier (URI). This URI does then embody the mapping of the different identifiers. In addition, it can also serve as a pointer
 - o to a document as described in the previous bullet,
 - o to provide information about the specific identifiers and identification schemes and/or
 - o to a proofing mechanism (e.g. a designated database as described above) which confirms the correctness of the mapping, i.e. that the different identifiers designate the same entity.

5.2.5 Requirements And Recommendations

Considering the explanations above, the following recommendations can be given for the insertion of unique business identifiers in electronic documents (the focus is on machine-readable documents):

- The identifier has to be given together with the identification scheme in the form of the URN notation (i.e. “urn:...”) if the context or document format does not define the usage of a specific identifier scheme (e.g. the GS1 EANCOM® profile for UN/EDIFACT messages mandates the usage of a GLN for the identification of locations).
- If possible, a business identifier shall be embedded in the URN under a registered formal namespace identifier. (See <http://www.iana.org/assignments/urn-namespaces/> for a list of registered URN namespace identifiers.)
- If a registered ICD value according to ISO/IEC 6523 exists for the identification scheme, the business identifier shall be meta-identified with this ICD value.
 - o In case that the business identifier is purely numeric (consisting of digits 0 to 9), the identifier should be embedded in a URN as an OID.
Example: urn:oid:1.3.2.552120784 denotes the SIREN (official French company identifier) 552120784. The ICD value of the SIRENE/SIREN system is 0002, which shows up in the URN as the trailing “2” of the OID “1.3.2”.
 - o Otherwise, the identifier may be embedded in a URN under the namespace “urn:oasis:names:tc:ebxml-cppa:partyid-type:iso6523”
Example: In
urn:oasis:names:tc:ebxml-cppa:partyid-type:iso6523:0169:CH-020.3.030.308-0 denotes the Swiss Commercial Register Number CH-020.3.030.308-0. The ICD value for Swiss Commercial Register Numbers is 0169.
 - o The workshop will apply for the registration of a URN namespace for iso6523 at IANA. The according procedures will be assessed and ISO/IEC JTC 1, “Information technology”, Subcommittee SC 32, “Data management services” (responsible for the ISO/IEC 6523 standard) will be contacted.
The reason for this step is that the URN shown in the previous bullet is rather lengthy. A URN of the type “urn:iso6523: 0169:CH-020.3.030.308-0” is easier to handle.

Concerning the mapping of unique business identifiers, the following recommendation can be given:

- An organization should publish a URL that points to a document which lists the relevant identifiers that identify this organization. It is recommended that this URL contains the according identifiers as URN's.

5.3. Verification Of Identifiers In Registries

5.3.1 Registration Criteria

The reliability of the information designated by an identifier depends mainly on the quality of the registration. This means that it has to be transparent to a relying party how the information about an entity in a register is verified by the registrar. Therefore, operational procedures are a key factor of organizational registration. For a systematic approach of the topic see ISO/IEC 6523-2 "Registration of organization identification schemes". The considered criteria for the evaluation of operational procedures are:

- (a) Criteria for Issuing Organizations allocating identifiers to business entities, i.e. for identification schemes of organizations and parts thereof
- (b) Criteria for meta-identifier registration of such identification schemes

Criteria for meta-identifier registration rely on the criteria for current identification schemes according to (a). The authority which issues meta-identifiers according to (b) relies on the documented and approved criteria for identifier allocation by Issuing Organizations.

- (a) Criteria for identification schemes of organizations and parts thereof

- Strength of the initial registration of the organization to be registered: the procedures contain registration rules for
 - Existence of an organization:
 - High: audited entry in an official registry, e.g. commercial registry, VAT registry, private or third party registry with vetting requirements in place etc.
 - Medium: presenting (sending copies of) receipts of phone bills etc.
 - Low: self-declaration, phone book entries
 - Responsible natural persons acting on behalf of the registered organization:
 - High: face-to-face registration (presenting official documents and signing of registration documents)
 - Medium: presenting (sending copies of) personalised documents, receipts of phone bills etc.
 - Low: un-audited self-declaration
 - Any registered attributes (e.g. ISO 9001 compliance, turnover values etc.):
 - High: Audit by an (accredited) third party
 - Low: un-audited self-declaration
- Renewal of registration:
 - High: periodic face-to-face renewal, re-auditing of registered attributes etc.
 - Medium: proof by paying periodic registration fees
 - Low: none
- Updates/changes of registered data:
 - High: contractual obligation of the registered entity to communicate any changes of its registered data
 - Low: none
- Publication of criteria:
 - A practice statement of applied criteria has to be available.

(b) Criteria for meta-identifier registration

In the context of this document only two criteria are relevant:

- Public statement of the responsibility of the registration authority for meta-identifiers
- Publication of the allocated meta-identifiers with a reference to the related criteria applied by the Issuing Organization

5.3.2 Recommendations

An Issuing Organization or registration authority must have a documented and publicly available policy for registration, renewal and updates (concerning the organization and all registered attributes). This policy must address the topics described in 5.3.1 "Registration Criteria".

5.4. Resolution Interfaces/Protocols And Services

5.4.1 Overview

Registers containing information about uniquely identified organizations must be accessible over the Internet when used in an open user environment. The same is true for redirection services, i.e. instances which redirect an identifier-resolving client to the proper register. Please note that the above mentioned two functions (provide register information and redirection) are not mutually exclusive, i.e. it is possible that a service answer can contain registration information and redirection instructions. E.g. a service can provide a register function concerning a company which is identified within the Organization Identifier (OI) of a unique identifier. In addition, it can offer redirection information as well concerning where to obtain data about the company unit that is specified in the Organization part Identifier (OPI).

These facts raise the question about which protocol-standards should be mandated or recommended in the application layer of the TCP/IP protocol suite (the Internet's network standards).

This chapter discusses the suitability of protocols for resolution considering the relevant aspects. These are:

Security:	How authenticity and integrity, as well as encryption (confidentiality, privacy and possibly access control) can be implemented with common means. Stress is laid on read-operations, i.e. the authenticity and integrity of server-messages.
Deployment:	Discussion of ease of deployment, i.e. complexity of implementation, if the usage of the protocol is compatible with common firewall policies etc.
Presentation flexibility:	Suitability of a protocol interface for different data presentation formats (esp. for human interaction besides automatic interaction) and for resolving multiple identifiers at once.
Performance:	This includes speed/latency, data payload (i.e. the format in which data is transmitted), caching and, as a result, scalability and availability.

At the end of this chapter 5.4, the according recommendations are given.

5.4.2 Domain Name System (DNS) Based Systems

Security:	DNSSec can guarantee authenticity and integrity. However, DNSSec is not widely implemented and does not provide encryption. Security could also be implemented on a lower protocol layer level (IPSec). When using DNS as redirection service, security can be implemented at the register. However, the according information for resolving the identifier is sent unencrypted when relying on the DNS only.
Deployment:	Deployment is simple as the DNS is a cornerstone of Internet usage. Therefore, also corporate firewalls are configured to allow DNS requests (UDP port 53) to the Internet.
Presentation flexibility:	DNS is a protocol not designed to transport documents. It is therefore apt for redirection services, but not as interface for registers. Due to the hierarchic structure of domain names the DNS is very apt to resolve single identifiers, but not to resolve multiple identifiers at once.
Performance:	DNS is optimised for low latency values and high volume in its default configuration (over UDP). Network performance is therefore very high. The DNS also contains a built-in caching mechanism.

5.4.3 Hypertext Transfer Protocol (Secure) - HTTP(S) Based Systems

Security:	Authenticity, integrity and encryption can be implemented by using HTTP over SSL/TLS, i.e. HTTPS. SSL/TLS is the most prevalent security protocol in the Internet and the usage within HTTPS its most common implementation.
Deployment:	Deployment is simple as the usage of HTTP based systems is widespread. Corporate firewalls are configured to allow requests to HTTP services (port 80) and most corporate firewalls are also configured to allow HTTPS requests (port 443).
Presentation flexibility:	<p>HTTP is designed to transport documents of any format (e.g. HTML for human-readability or XML for automatic processing). HTTP also specifies the according header-information (Accept or Content-Type) which allows clients to state the preferred data-format and servers to announce the transmitted data-formats.</p> <p>The protocol also allows the lookup/resolving of multiple identifiers at once, e.g. by embedding them into an HTTP(S)-URI.</p>
Performance:	<p>The mitigating factor for network performance is that HTTP is run on top of the TCP-protocol. It can therefore not achieve the volume of UDP based protocols as TCP is optimized for accurate delivery which involves the exchange of control messages which results in reliable but slowed exchange of data packets.</p> <p>Also, the impact of using SSL/TLS for security on the computing performance is considerable.</p> <p>There are no restrictions concerning the data payload transported.</p> <p>HTTP has a built-in caching mechanism.</p>

5.4.4 Lightweight Directory Access Protocol (Secure) - LDAP(S) Based Systems

Security:	Authenticity, integrity and encryption can be implemented by using LDAP over SSL/TLS, i.e. LDAPS. LDAPS is commonly used.
Deployment:	Most corporate firewalls allow LDAP-requests (port 63). LDAPS-requests (port 636) might be blocked by corporate firewalls.
Presentation flexibility:	LDAP is designed for directory querying. It is specified as exchanging ASN.1 messages. Identifiers can be included in the attributes part of an LDAP-URI.
Performance:	The usage of BER-encoded ASN.1-messages minimises the network traffic of LDAP. The mitigating factor for network performance is that LDAP is run on top of the TCP-protocol. It can therefore not achieve the volume of UDP based protocols. Also, the impact of using SSL/TLS for security on the computing performance is considerable.

5.4.5 SOAP And ebXML Messaging Services (ebMS) Based Systems

Please note: The ebXML Messaging Services (ebMS) Specification specifies rules for exchanging electronic business messages. ebMS is layered over the SOAP-protocol; therefore, analogous statements about SOAP and ebMS can be made.

Security:	There are well defined standards for signing (authenticity and integrity) and encrypting SOAP messages.
Deployment:	SOAP is designed to be "protocol-independent", i.e. SOAP can be run over any other application layer protocol or over a transport layer protocol like TCP or UDP. In practice, SOAP is usually running on top of HTTP or HTTPS. Therefore, similar statements concerning corporate firewall permeability as for HTTPS can be made. However, it is possible that firewalls doing packet inspection block SOAP messages.
Presentation flexibility:	Messages can take any file-formats as payload.
Performance:	Performance is dependant of the underlying protocol. The impact of the usage of XML has also to be considered.

5.4.6 Comparison Of Different Protocols

Considering the outlining above under the aspects of security, deployment, presentation flexibility and performance, the strengths and weaknesses of the according interfaces can be quantified and compared under these aspects. This comparison is best presented as a matrix. This matrix is shown below.

The scale chosen ranges from 1 (+) designating the low end to 5 (+++++) designating the high end. Please note that this scale is relative, i.e. only valid for the comparison of the described set of protocols.

Interface Aspect	DNS	HTTP(S)	LDAP(S)	SOAP/ebMS
Security:	++	+++++	+++++	+++++
Deployment:	+++++	++++	+++	+++
Presentation flexibility:	+	+++++	++	+++++
Performance:	+++++	+++	++++	++

The conclusion of this comparison is the following: As one would expect, the protocols to be used for access to a register depend on the specific needs. However, the most flexible approach is to use the HTTP protocol (with the possible combination with SSL/TLS - HTTPS).

HTTP for accessing web-applications/web-services using the according commands as they are specified in chapter 9 of IETF RFC 2626 has also increased in acceptance and coverage in the last years. This approach is referred to as “REST” (REpresentational State Transfer) based Web-Services.

5.4.7 Specific Applications

The Global Electronic Party Information Register (GEPIR - GS1 member directory), the French National Institute for Statistics and Economic Studies (INSEE), Dun & Bradstreet, the Swiss Central Business Index and many other Issuing Organizations provide a public interface to their registers over HTTP. The according information is always provided in at least the HTML-format. Some registers provide a presentation of the data in the XML-format for automatic processing.

Two technical implementations for automated exchange have to be mentioned specifically:

The ebXML Registry³⁴ technology provides a set of services that enable sharing of information between interested parties for the purpose of enabling business process integration between such parties. The ebXML Registry Services Specification describes the according interfaces. An ebXML Registry can be accessed via SOAP binding.

An example of a public ebXML registry is the one provided by the Korea Trade Network.

Universal Description Discovery & Integration (UDDI)³⁵ is a registry interface implementation which defines a set of services supporting the description and discovery of organizations and their Web services (including the specific interfaces). A UDDI can be accessed via SOAP binding. The UDDI specification describes in Appendix E how unique business identifiers may be used to access a UDDI.

A specification of an OID (compare chapter 2 “OID According To ISO/IEC 9834-1” in 5.2.2 “Inventory”) resolution system is drafted at the time of the writing of this CWA in ITU-T SG 17 and ISO/IEC JTC 1/SC 6 (draft ITU-T X.oid-res | ISO/IEC 29168). This will very probably be a DNS-based system which will provide information about an OID.

³⁴ OASIS/ebXML Registry Services Specification v3.0.1

³⁵ OASIS UDDI Version 3.0.2

5.4.8 Community Of Resolution Services

Interoperability:

In order to achieve interoperability of unique business identifiers (as described in 5.2.3), two approaches exist in theory: a centralised world-wide system with one standardised unique identifier and a federation approach. In practice, only the federation approach is feasible as different identification systems are well established in autonomous domains of control and because this diversity will continue in the future. In order to assure low administrative effort and a maximum flexibility of using and verifying organization identification schemes, an approach which favours federated solutions and minimising hierarchical structures has to be applied. This approach allows all actors in an open environment to build connections and alliances while keeping their independence and flexibility. They remain independent with respect to strategic decisions and flexible in the implementation of their business models and processes.

Federation:

The term federation denotes standards of operation that allow data sharing of multiple, independent, self-governing providers without affecting their applications. Within the context of this document, the providers operate a resolution service for unique identifiers, i.e. a

- registry/directory which can be accessed via a unique identifier as key
- and/or a redirection service for unique identifiers.

A redirection service works only by means of an explicit or implicit meta-identification of the identifiers it redirects to. A harmonised, federated system of resolution services hence depends on agreed standards for meta-identification.

Therefore, meta-identification is key to interoperability and an agreement on meta-identification is a necessary condition for interoperability.

Trust:

The explanations concerning federation and resolution services given above describe the technical and logical aspects of the topic. An additional dimension is given by the fact that an actor within such a system has to trust the according resolution service. This trust is driven by its policies (in writing or based upon commercial duty or good reputation). These policies may rely on the according registration criteria as described in chapter 5.3.1. Therefore, federation/community of resolution services is not only a matter of technical implementation, but also a matter of trust. A resolution service enforces trust between parties and facilitates interaction between these parties. An entity that performs this function is called a Trusted Third Party (TTP).

Therefore, the federation mechanism sets up a chain of trust between

- | | |
|------------|--|
| (ver) | the verifier of the specified business identifier who trusts |
| (TTP) | a Trusted Third Party which accepts/recognises/accredits |
| (dir) | the register/directory managed by a specific provider containing |
| (info) | the information specified by the business identifier ID and |
| (ID-owner) | the owner/licencee of the business ID. |

Please note: the provider of the directory and a Trusted Third Party can be the same organization.

Either the *verifier* trusts the operator of the directory directly (ver) → (dir) or the *verifier* trusts a *Trusted Third Party* (TTP – compare 3.1 “Definitions”) which in turn trusts the operator of the directory i.e. (TTP) → (dir).

Any system providing interoperability has to show how a verifier (ver) can check or rely on information (info) specified by a business ID by following this *Chain of Trust*. The link between the (TTP) Trusted Third Party and the (dir) register/directory depends also on the meta-identifier allocated to the specific register/directory by the specific Trusted Third Party. Thus the core of such a system is a (formal or tacit) agreement on meta-identification between the verifier and the owner of the business ID.

The conclusion is: A formal or tacit agreement on meta-identification is a prerequisite for interoperability between identification schemes.

The verifier (ver) checks or relies on information (info) specified by a business ID by following this *Chain of Trust*. The verifier has to trust the specified Trusted Third Party (TTP). However, what has to be done if the verifier does not know the included TTP?

Obviously a system is needed which allows to set up a trust link between trusted third parties. Such a trust link can be bidirectional or may be only unidirectional. Example based on the following trust links:

$TTP_1 \leftrightarrow TTP_2$ TTP_1 trusts TTP_2 and vice versa

$TTP_1 \leftarrow TTP_3$ TTP_3 trusts TTP_1 but not vice versa

$TTP_1 \leftrightarrow TTP_4$ TTP_1 trusts TTP_4 and vice versa

- TTP_1 has to show its trust links $TTP_1 \rightarrow TTP_2$ and $TTP_1 \rightarrow TTP_4$
- assuming the verifier (ver) does not know TTP_1 but (ver) knows and trusts TTP_4
- then the trust chain (ver) $\rightarrow TTP_1 \rightarrow TTP_4 \rightarrow$ (dir) \rightarrow (info) specified by the ID becomes viable, i.e. is complete because (ver) trusts TTP_4 .

The prerequisite (in this example) is: the ID to be verified shows the following relationships $TTP_1 \rightarrow$ (dir) \rightarrow ID as well as $TTP_4 \rightarrow$ (dir) \rightarrow ID in a standardised form. Following the implied chain of trust is called *resolution* of an ID (including meta-identification).

Thus any owner of a specific ID who wants the related information to be made visible/checkable on an electronic document has to append the unique ID of a business entity in such a standardised form:

$TTP_i \rightarrow$ (dir) \rightarrow ID

TTP_i using a specific meta-identification scheme and showing its trust links with other TTPs;

The necessary Internet standards are available (see the above discussed protocols). Based on these standards a community of resolution services for IDs can be set up by Trusted Third Parties (TTPs) and directory services.

5.4.9 Technical Security Criteria

On the technical level, security is the most important issue. A comprehensive security strategy cannot be described by a set of simple rules. But it comprises the proper documentation of security management measures. Directions concerning this topic can be found in ISO/IEC 27001 "Information security management systems – Requirements" and ISO/IEC 27002 "Code of practice for information security managements". Please note that a certification according to these standards is possible but not mandatory.

5.4.10 Requirements And Recommendations

The following is recommended for providers of resolution services for unique identifiers:

- Register interfaces must be available over HTTP. These interfaces may also be available over HTTPS. (Please note that this does not preclude the parallel support of other protocols for resolution.)
- It must be possible to make a query over HTTP with an identifier as input.
- Queries for identifiers should be possible with the HTTP GET method (in accordance with chapter 9 “Method Definitions” of IETF RFC 2616)
- A register provider must offer an interface in HTML/XHTML.
- It is recommended that register providers offer a machine-readable interface in the XML-format. (Please note that this does not preclude the parallel support of other formats.)
- A register service provider must publish an OpenSearch description file that specifies the URL's for identifier-queries over HTTP and/or HTTPS. The description must contain a URL for an HTML-interface. If additional interfaces are available, the description must contain the according URL's as well.
Please consider chapter 6.1.8 for more information about OpenSearch.
- It is recommended that registers publish at least minimal information (such as an organization's name) free of charge.

6. Part 3: Use Cases And Specific Issues

6.1. Technologies In Use

6.1.1 Introduction

Within this section, different technologies are discussed under the perspective of unique (business) identification and verification of identifiers. Uniform Resource Identifier (URI) and OpenSearch are discussed as they can or do support means for unique identification and its verification. PKI, UN/EDIFACT, UBL and ebXML are discussed under the aspect of how these technologies can rely on unique business identification and can therefore take benefit of coordination and recommendation actions in the area of unique (meta-)identification and its verification.

6.1.2 URI

The Uniform Resource Identifier (URI) concept stems from the objective of defining a unifying syntax for the expression of names and addresses of objects on the network as used in the World-Wide Web. The web is considered to include objects accessed using an extendable number of protocols, existing, invented for the web itself, or to be invented in the future. Access instructions for an individual object under a given protocol are encoded into forms of address string. Other protocols allow the use of object names of various forms.

Internet users are already familiar with the URL syntax, which is a subset of URI in as much as it expresses an address, which maps onto an access algorithm using network protocols already operating on the web. URIs, which refer to objects accessed with existing protocols are known as "Uniform Resource Locators" (URLs). More generally a Universal Resource Identifier (URI) aims to give rules for this universal set of names in registered name spaces and addresses referring to registered protocols or name spaces. More specifically, a Uniform Resource Name (URN) attempts to define a name space (and presumably resolution protocols) for persistent object names.

Many protocols and systems for document search and retrieval are currently in use, and many more protocols or refinements of existing protocols are to be expected in a field whose expansion is explosive. This is the reason why these systems are aiming to achieve global search and readership of objects across differing computing platforms, and despite a plethora of protocols and data formats. As protocols evolve, gateways can allow global access to remain possible. As data formats evolve, format conversion programs will preserve global access.

A common feature of almost all the data models of past and proposed systems is something which can be mapped onto a concept of "object" and some kind of name, address, or identifier for that object. One can therefore define a set of name spaces in which these objects can be said to exist.

Practical systems need to access and mix objects which are part of different existing and proposed systems. Therefore, the concept of the universal set of all objects, and hence the universal set of names and addresses, in all name spaces, becomes important. This allows names in different spaces to be treated in a common way, even though names in different spaces have differing characteristics, as do the objects to which they refer.

In this context, the URI initiative aims to define a way to encapsulate a name in any registered name space, and label it with the name space, producing a member of the universal set. Such an encoded and labelled member of this set is known as a Universal Resource Identifier, or URI.

The specification of the URI syntax does not imply anything about the properties of names and addresses in the various name spaces which are mapped onto the set of URI strings. The properties follow from the specifications of the protocols and the associated usage conventions for each scheme.

The following approach is currently considered. Uniformity provides several benefits and allows different types of resource identifiers to be used in the same context, even when the mechanisms

used to access those resources may differ. The specification³⁶ does not limit the scope of what might be a resource; rather, the term "resource" is used in a general sense for whatever might be identified by a URI. Finally, the term "identifier" embodies the information required to distinguish what is being identified from all other things within its scope of identification. Our use of the terms "identify" and "identifying" refer to this purpose of distinguishing one resource from all other resources, regardless of how that purpose is accomplished.

6.1.3 IRI

Internationalized Resource Identifiers (IRIs) are a superset of the Uniform Resource Identifiers (URIs) described above. While a URI can only contain characters of the restricted American Standard Code for Information Interchange (ASCII) character set, an IRI can contain characters from the Universal Character Set (UCS). The IRI concept is described in IETF RFC 3987 "Internationalized Resource Identifiers (IRIs)".

6.1.4 PKI

Concerning the implementation of Public Key Infrastructures (PKI) and its advantages, flaws, opportunities and subsequent risks, one has to consider if the implementation is for targeting a closed or an open user group.

The characteristics of a closed user group involve the fact that the interacting parties know each other beforehand and thus may use additional conventions to process certificates inside the closed user group. The process to identify an organization /or its part may be standardised among the closed user group. This additional process is however unknown in open user groups.

On the other hand, within open user groups, actors do not exercise business relationships before exchanging certificates. Therefore, the receiver of a certificate faces the problem to identify an organization or its part within a certificate. This may be done in two steps: (a) retrieving appropriate information from the certificate, and (b) using it when accessing a trusted data base in order to get more details about the organization.

The common ways to identify a certificate-holder (or more precisely "the entity associated with the public key stored in the subject public key field"³⁷) in an X.509 certificate are:

- the "Subject" field:

This field usually (if not empty) contains a "Distinguished Name" (DN) which is a hierarchically built name of the certificate holder, e.g. the residence country, the organization of the certificate-holder, the organisation unit to which the certificate-holder belongs to and the holder's name. Such a Distinguished Name must be unique for the certified entity within the domain of the issuing CA. However, in the general case, the choice of DN components is left open.

Some recommendations have been made in section 3.1.1 from RFC 3739 (Qualified Certificates Profile) to identify a certificate issuer (which is an organisation). In such a case, the distinguished name of the issuer shall be specified using an appropriate subset of the following attributes:

- domainComponent;
- countryName;
- stateOrProvinceName;
- organizationName;

³⁶ See <http://tools.ietf.org/html/rfc3986>

³⁷ [IETF RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile"](#)

- localityName; and
- serialNumber.

The organizationName should be an officially registered name of the organization.

RFC 5280 recommends that names should not be reused for different entities and thus certificates do not need to make use of the field subject UniqueID to distinguish between different entities that would otherwise have the same DN. For that reason, the use of subject UniqueIDs (as well as issuerUniqueIDs) is deprecated by RFC 5280.

- an eMail address:

An eMail address according to RFC 5280 should be part of the "Subject Alternative Name" extension. Simultaneous inclusion of the email Address attribute in the Subject Distinguished Name to support legacy implementations is deprecated but permitted and still done by several Certification Service Providers (CSP's). The eMail address allows identifying the mail box of an individual or the mail box of a service.

eMail addresses are sometimes used to uniquely identify an entity designated in an X.509 certificate. A problem of this approach is that such eMail addresses are not persistent and do therefore not guarantee a stable association with the certified entity over time. E.g. the eMail address john.doe@large-company.test does not necessarily designate the same employee today as it did two years ago. From an operational point of view, the inclusion of eMail addresses in certificates is an obstacle when an organization or organizational unit has to update its domain name, e.g. as a consequence of a reorganization or of a re-branding. eMail addresses are rarely or never used to query registers in order to track business data.

- Organization Unit Name:

The Distinguished Name component "organizationUnitName" is sometimes used for the inclusion of unique business identifiers. See the use case "French governmental General Security Framework" in "6.2.2 X.509 Public-Key And Attribute Certificates".

- The "Serial Number" attribute:

The Distinguished Name component "serialNumber" is sometimes used for the inclusion of unique business identifiers. See the use case "Extended Validation SSL Certificates" in "6.2.2 X.509 Public-Key And Attribute Certificates".

NOTE The "Serial Number" attribute should not be confused with the mandatory field of the same name in an X.509 certificate which specifies a unique number for every certificate issued by a Certification Authority (not for the certified entity which may be associated with more than one certificate). The "Serial Number" attribute is a naming attribute defined in the X.520 specification and is supported by applications conforming to IETF RFC 5280 and its predecessors. It is therefore supported by the common applications for processing X.509 certificates.

The problems of using the Serial Number attribute for the inclusion of unique business identifiers can be described as follows:

An important observation can be made: several times the semantics of the SerialNumber has been changed by certificate issuers in closed user groups. When a serialnumber component is used in a DN, its primary purpose is to differentiate between names where the subject field would otherwise be identical. It is the CA's responsibility to ensure that the serialNumber is sufficient to resolve any subject name collisions.

This attribute has no defined semantics beyond ensuring uniqueness of subject names.

The SerialNumber attribute may only take an additional semantics and thus be used for other purposes, if other information allows adding such an additional semantics. This is typically the case with RFC 4043 which places a specific additional extension in the certificate itself to say so. This approach is usable in an open user group.

This is also the case, if when validating a certificate, it may be discovered that the certificate carries some additional property. This is typically the case for EV SSL Certificates, where once it is been verified that the certificate is a EV SSL Certificate (which mandates the construction and the validation of the certification chain) an additional semantics can be given to SerialNumber attribute included in the EV SSL Certificate.

- The “Permanent Identifier” as defined in RFC 4043:

It includes two components that shall be placed into a specific field from the Subject Alternative Name to uniquely identify the certificate holder: the identifierValue field and the assigner field which are both optional, but at least one of them must be present.

When the assigner field is present, then it is an OID which identifies a naming space, i.e., both an Assigner Authority and the type of that field. Characteristically, the prefix of the OID identifies the Assigner Authority, and a suffix is used to identify the type of permanent identifier.

When the assigner field is absent, then the permanent identifier is locally unique to the CA.

When the identifierValue field is present, then the identifierValue supports one syntax: UTF8String.

When the identifierValue field is absent, then the value of the serialNumber attribute (as defined in section 5.2.9 of [X.520]) from the deepest RDN of the subject DN is the value to be taken for the identifierValue.

When the certificate holder is an organisation, the Permanent Identifier allows uniquely identifying an organisation. When the certificate holder is an employee, the Permanent Identifier allows uniquely identifying the employee, but not the organisation he works for.

It should be remembered that without using a unique identifier, there is a risk that the same Subject Distinguished Name certified by two different CA's do not designate the same entity. The variety in the composition of such a name also hampers the automatic processing of it. As most of the parts of DN have human readable values, the DN is not necessarily persistent over time. (E.g. a company that is specified in the “organization” part of the DN might change its name after being acquired.) A possible new approach would be the following:

DN attributes, as currently defined, do not allow incorporating a DN attribute that would carry a unique business identifier for an organization. The lack of such an attribute leads to shortcut solutions like using the serialNumber attribute or using an organization unit attribute (see the use case in section 6.2.2 about the French governmental general security framework). A better solution would be to define a new DN attribute (e.g. called “Organization Identifier” – OI) that would include a value structured as defined in ISO/IEC 6523. Since the DN attributes have been originally defined by JTC 1/SC 6/WG 8 in charge of the Directory, such a standardization work would be undertaken by this working group. If this approach is followed, an addendum to ITU-T X.520 | ISO/IEC 9594-6 would be made”.

Having said the above, the requirements for the inclusion of unique business identifiers for organizations and parts thereof in X.509 certificates can be deduced. A solution for this issue should match the following requirements:

- There should be a way to designate a field and/or component from a field in public key certificates for including unique identifiers and an agreed format for these unique identifiers.

Note that there already exists a solution for such a designation when the certificate holder is an organization (see RFC 4043), but not when it is an employee working for an organization.

- The unique identifiers to be used must be persistent over time. The structure defined in ISO/IEC 6523 should be considered.
- The unique identifiers should be verifiable, i.e. it should be possible to (automatically) track business data associated with the designated entity. The addition of URLs pointing to some data base or registry should be considered.

More general information about PKI is given in the section “A.1 PKI” of “Annex A (Informative): Background”.

6.1.5 UN/EDIFACT

Concerning the exchange of messages according to United Nations Electronic Data Interchange For Administration, Commerce, and Transport (UN/EDIFACT) the following two aspects regarding unique business identifiers have to be considered separately:

1. The usage of identifiers in the messages themselves. The existing (well-established) sector-specific specifications – the so called “UN/EDIFACT subsets” – each address the topic in their own way: E.g. GS1 EANCOM® requires the usage of GLNs. Generally speaking, the relevant meta-identification is defined by the context itself.
2. The transport, including the routing of these UN/EDIFACT messages, is traditionally performed over Value Added Networks (VAN's). In addition the Internet, as a communication infrastructure, has created new and cost-effective ways for the transport of UN/EDIFACT messages: Prominent examples are the “Applicability Statement 2” (AS2) as specified in IETF RFC 4130 “MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)” or the Odette File Transfer Protocol (OFTP) version 2 as specified in IETF RFC 5024. These protocols specify mandatory fields to (uniquely) identify both the sending and the receiving system.

ISO/IEC

The chapter 6.2 “AS2 System Identifiers” of IETF RFC 4130 specifies which fields of AS2 must be included in the message exchange as the HTTP headers “AS2-From” (for the sender) and “AS2-To” (for the receiver). This chapter gives several examples of what kind of identifiers may be used but does not mandate the use of a specific identification or meta-identification scheme. IETF RFC 5024 “ODETTE File Transfer Protocol 2” describes the format of these fields in section 5.4 “Identification Code”. This format requires the use of International Code Designator (ICD) values according to ISO/IEC 6523 (compare 5.2.2) for meta-identification of the identification scheme used to identify the organizations’ system.

6.1.6 UBL And GENERICODE

The “Universal Business Language” (UBL) is a set of standardised XML-based vocabularies for business documents in the order-to-invoice cycle. The current 2.0 version of UBL is maintained by the OASIS Universal Business Language Technical Committee. UBL makes an extensive use of the concept of identifiers to relate to business data.

Since the 2.0 version, UBL relies on Genericode for identifiers currently used as references, i.e. which are symbolic representational keys for human-readable values.

EXAMPLE: An enumeration of currency codes is stored in a separate Genericode list. This has the advantage that the inclusion of a new currency and its code does not require a UBL-schema-definition (the vocabulary) to be updated. It also facilitates the multilingual representation of a UBL document and enables

the versioning of an identifier-update. Genericode is based on a tabular data model (as known from relational databases).

From the point of view of unique business identifiers the UBL data elements CompanyID, PartyIdentification ID, EndpointID and CorporateRegistrationScheme are of great interest:

- CompanyID represents an official business register/commercial registry identifier or a VAT number.
- The PartyIdentification ID is an identifier for a party involved in a transaction (usually the seller or the buyer).
- EndpointID represents the identification of an endpoint of a routing service.
- CorporateRegistrationScheme associates the party with a Corporate Registration Scheme.

Example of usage:

```
<cac:PartyIdentification>
  <cbc:ID schemeID="DK:CVR">DK45656787</cbc:ID>
</cac:PartyIdentification>
```

The meta-identification of the identification scheme is provided by the value "DK:CVR" of the attribute "schemeID" of the ID-tag. "DK:CVR" designates the identification scheme of "The Danish Commerce and Companies Agency" (The central commercial registry of Denmark). "DK45656787" would be the specific commercial registry number assigned to a specific Danish company.

While the content of the CompanyID element is specified by the effective legal requirements, both the contents of PartyIdentification ID and EndpointID are subject to bilateral agreements or of a general policy correspondingly. Such a policy facilitates the establishment of a new trade relationship and the exchange of UBL documents between the partners respectively.

6.1.7 ebXML

ebXML stands for electronic business using eXtensible Markup Language. It is a family of XML based standards sponsored by the "Organization for the Advancement of Structured Information Standards (OASIS)" and United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). Its purpose is to provide an infrastructure that enables interoperability between all trading partners concerning the exchange and use of electronic business information. Therefore, the scope of ebXML is rather wide. It comprehends

- Business processes,
- Collaborative Partner Profile Agreement (CPPA),
- Core data components,
- Messaging (ebMS - compare also 5.4.5 "SOAP And ebXML Messaging Services (ebMS) Based ")
- and Registries and repositories (compare 5.4.7 "Specific Applications").

Five of the according specifications have been released as ISO standards (ISO 15000 parts 1 - 5).

Besides the ebXML Registry specification, "Collaborative Partner Profile Agreements (CPPA)" and the specification concerning messaging are of special interest from the perspective of unique identification. "Collaborative Partner Profile Agreement" specifies an XML based vocabulary for creating documents describing eBusiness relevant trading partner data. Each trading partner maintains its own "Collaboration Protocol Profile" and out of the intersection results an agreement document. Besides, it contains technical and process-related information for the unique identification of partners and their respective roles in the business relationship. The "ebXML

Message Service Specification (ebMS)” is a SOAP based specification for enveloping and exchanging business documents. Both specifications mandate the association of the involved parties with one or more identifiers and rely for this on the so-called “PartyID” element.

EXAMPLE 1:

```
<tp:PartyId tp:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:D-U-N-SNumber:0060">
    123456789
</tp:PartyId>
```

EXAMPLE 2:

```
<tp:PartyId>
    urn:oasis:names:tc:ebxml-cppa:partyid-type:D-U-N-SNumber:0060:123456789
</tp:PartyId>
```

The two examples show the format of the “PartyID” element and how unique business identifiers have to be included in it. In example 1 the meta-identification scheme is included as value in the “type” attribute of the element and its corresponding unique identifier is included in the body of the “PartyId” tag. The value of the “type” attribute needs to be a Uniform Resource Identifier (URI). In example 2 the “type” attribute is omitted. The body of the “PartyId” tag has therefore to contain an identifier as a URI. In both examples a Uniform Resource Name (URN) under the registered namespace “oasis” is used to meta-identify the D-U-N-S[®] number as identification scheme. Concerning the identification schemes the ebXML CPPA suggests to rely on the D-U-N-S[®] number or any other ISO/IEC 6523 registered identification scheme. It states further: *“It is RECOMMENDED that the value of the type attribute be a URN that defines a namespace for the value of the PartyId element. Typically, the URN would be registered in a well-known directory of organization identifiers.”*

6.1.8 OpenSearch

OpenSearch stands for a collection of simple XML-based formats for the sharing of search results. The most important of these formats is the “OpenSearch description document” which provides a standardised vocabulary to describe the interface(s) of a search engine (or any database accessible over HTTP or FTP). Examples of search clients that support OpenSearch description documents are the browsers Mozilla Firefox 2.0 and MS Internet Explorer 7.0 and above. In these browsers, the search bar (located in the upper right of the window) can be populated with the interfaces of OpenSearch description files. In addition to these examples that show the possibilities for querying and displaying human-readable content, the vocabulary is designed for any kind of machine-readable structured content as well.

This vocabulary is therefore entirely suited for describing how registries can be queried, e.g. with an unique business identifier as input.

More information about OpenSearch can be found on <http://www.opensearch.org/>. The corresponding specifications are licensed under a Creative Commons license.

6.2. Use Cases

6.2.1 Introduction

The chapter 6.1 “Technologies In Use” lists a choice of technologies that are important when it comes to contributing to or benefiting from (harmonised) unique identification systems. It shows the issues and questions that arise concerning the application of unique business identification within these technologies.

The chapter 6.2 “Use Cases” is dedicated to how the issues can be solved. Where possible specific recommendations are given using the findings of chapter 5 “Part 2: Inventory Of Applications And Associated Requirements”. The following Use Cases do not make up a comprehensive list of applications using unique business identification. It is rather a selection of significant and promising examples which also demonstrate that the findings of Part 2 can be used in different important application areas. Therefore, it also contains new applications benefiting from harmonised unique business identification like 6.2.7 “Trustlabels” and 6.2.8 “Presentment Of Conformity Assessment Certificates”.

6.2.2 X.509 Public-Key And Attribute Certificates

Extended Validation (EV) SSL Certificates

An example of the inclusion of identifiers for organizations in the “Serial Number” attribute are the so called Extended Validation (EV) SSL Certificates. EV SSL Certificates are certificates issued according to the “Guidelines for the issuance and management of Extended Validation Certificates”³⁸ of the CA/Browser Forum. The CA/Browser Forum consists of the leading browser manufacturers and of several Certification Service Providers. The goal of the EV SSL Certificate guidelines is to reach a higher level of trust for EV SSL Certificates than for traditional SSL/TLS (Secure Socket Layer/Transport Layer Security) certificates. This is done by setting high requirements for these certificates concerning registration, content and cryptography. Modern browsers allow distinguishing EV SSL Certificates from other SSL/TLS certificates by changing the background to green of a part or of the entire address bar. Technically, for discovering that a certificate is an EV SSL Certificate, it is necessary to build and validate a certificate chain starting from a Trust Anchor that uses a CP OID that has a given value known in advance.

The EV SSL guidelines require that a Registration Number is included in “Subject Distinguished Name” of the certificate as a “Serial Number” and states for the content:

“For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate.”

This means that usually a Commercial Registry Number of the organization has to be incorporated in the certificate. However, some jurisdictions do not stipulate the operation of Commercial Registries and therefore another identifier is inserted. It also happens in practice that a D-U-N-S® number is included instead of a Commercial Registry Number. It might remain therefore unclear what kind of identifier was incorporated and where to find the register where it can be checked. A proper meta-identification of the corresponding numbers is currently missing but would be useful.

French Governmental General Security Framework

In a document co-issued by the French DCSSI and the French Ministry of Finances³⁹, section VII.2.1 allows to uniquely identify the organisation an employee belongs to. This document was initially started about ten years ago. The goal was to include a unique identifier that would be visible using common web browsers. The solution chosen at that time was to include the

³⁸ See <http://www.cabforum.org/documents.html>

At the time of the writing of this CWA this specification has been proposed to the ITU-T for adoption as Recommendation ITU-T X.5cert.

³⁹ http://www.references.modernisation.gouv.fr/sites/default/files/RGS_Profils_Certificat_LCR_OCSP_V2_2.pdf

« Référentiel Général de Sécurité Politiques de Certification Types Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques » Version 2.2, issued on November 14, 2008.

information in the DN. Since it is not allowed to have more than one DN component of the class “Organisation” in a DN to identify an organisation, the choice was to use an organizationUnitName component immediately following the organizationName component to carry that information.

It has been decided to structure the content of this DN component according to ISO/IEC 6523 (“Structure for the Identification of Organisations (SIO)”). This is a syntax for uniquely identifying organizations in computer data interchange. It is composed of:

- 4 digit ICD (International Code Designator), which uniquely identifies the authority which issued the code to the organisation,
- an organisation code, up to a maximum of 14 characters (A-Z, 0-9, space or hyphen).
- An organisation name, up to a maximum of 250 characters

In this document, the structure has been refined in the following way:

For French organisations, the ICD must have the value 0002 and the organisation code must either be:

- a space character, followed by the SIREN code (9 characters), or,
- the number of the SIRET code (14 characters).

For foreign organisations, there exist two options:

- the DN Component of the class organizationUnitName starts with four digits, but these four digits are different from the value 0002. This denotes an identification scheme not using a SIREN or a SIRET number.
- the DN Component of the class organizationUnitName is not conformant to ISO/IEC 6523. In such a case, it MUST NOT start with 4 digits.

If other instances of DN Component of the class organizationUnitName are present, they MUST NOT start with 4 digits.

In any case, there is no organisation name present in this DN component (since it is already present in the DN component of the class “Organisation” in the DN).

6.2.3 eInvoicing

The CWA 15576 “Recommendation to allow coded identifiers as an alternative to the current unstructured clear text identifications”⁴⁰ discusses the following problem: It is an established practice in (automated) eInvoicing (and eProcurement in general) that the trading parties – of course including the taxable person – are represented by unique identifiers. In addition, products and services are designated by unique identifiers and qualified by classification codes. The VAT Directive 2001/115/EC (and the updated version 2006/112/EC) state requirements for the content of an invoice. This includes “the full name and address of the taxable person and of the customer” and “the quantity and nature of the goods supplied or the extent and nature of the services rendered”. These general requirements are valid for all invoices – for paper-based and electronic ones – and do not differentiate concerning the utilised medium.

Several EU member countries do therefore allow the usage of coded identifiers instead of clear text in electronic invoices, provided that look-up tables are available when required for inspection. However, some member states that do not have a long experience with eBusiness do not allow this.

⁴⁰ See <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eInvoicing/CWA15576-00-2006-Jul.pdf>

CWA 15576 therefore proposes a possibility how the VAT Directive could be updated in order to make clear that the usage of unique identifiers instead of clear text should be allowed in electronic invoices. In addition, it contains a list of examples of possible identifier schemes. It further makes the recommendation to develop Best Practices concerning the application of unique identifiers for eInvoicing:

“4.5.2 Best practice procedures

The CEN eInvoice Workshop is recommending that ‘Best practice procedures’ be made available to assist in developing applications, both for traders and VAT administration, that reflect the requirements of the VAT Directive and the eBusiness applications of today, taking the issue of coded identifiers into consideration, especially for cross border trade.”

Such Best Practices should contain recommendations about the requirements for the identification schemes to be used, especially concerning the registration criteria. Therefore, the recommendations given in 5.3.1 “Registration Criteria” should be taken into account.

More general information about eInvoicing is given in the section “A.2 eInvoicing” of “Annex B (Informative): Questionnaire For Issuers Of Unique Identifiers”.

6.2.4 UBL

As described in 6.1.6 the “Universal Business Language (UBL)” specification contains several elements that hold unique identifiers for organizations and parts thereof. Within a community that uses UBL for the exchange of business documents, a consensus on identification schemes to be used must exist. In addition, the labelling of the meta-identifiers needs to be standardised.

An example can be found in the chapter 3 of the “NES Code Lists and Identification Schemes”⁴¹. NES stands for Northern European Subset and is a cooperation for facilitating and implementing electronic procurement (with representatives from Denmark, Sweden, Norway, Finland, Great Britain and Iceland). The main focus is on the customisation of the UBL standards.

The mentioned code list document enumerates in chapter 3 the allowed possibilities of identification schemes to be used in the NES-UBL community for “Endpoint ID” and “Party ID”/PartyIdentification ID. In addition, the lists mandate how identification schemes have to be meta-identified (by the corresponding values in the “schemeID” attribute). Among the allowed schemes, one can cite national governmental identification schemes, IBAN, D-U-N-S®, GLN and any ISO/IEC 6523 registered scheme.

From this specific example general recommendations for UBL communities can be given:

Recommendations

- A UBL community should specify a list of allowed identification schemes to be used in the “EndpointID” and “PartyIdentification ID”. This list must include the relevant indications of meta-identification in the “schemeID” attribute.

6.2.5 ebXML Messages / ebXML CPPA

As described in chapter 6.1.7, The ebXML messaging specification (ebMS) and the ebXML Collaborative Partner Profile Agreements (CPPA) demand the usage of the “PartyID” element for the unique identification of business parties with a Uniform Resource Identifier (URI) as (meta-) identifier.

⁴¹ See <http://www.nesubl.eu/download/18.6dae77a0113497f158680002577/NES+Code+Lists+and+Identification+Schemes+-+Version+2.pdf>

The ebXML messaging specification has been implemented in practice in different sectors, e.g. for eGovernment applications, in the health sector or the automotive industry. As these applications are mostly used by user groups of manageable size and geographical range, the corresponding values for the “PartyID” elements are scheduled by the policy of the provider of the ebMS infrastructure.

However, when such networks expand, make connections and grow together, the different providers need a common policy concerning which unique business identifiers can be used. It is therefore necessary to agree on basic requirements for these identifiers and provide the corresponding recommendations for the values of the “PartyID” element to be used in ebMS and ebXML CPPA:

Recommendations

- The URI to be included in the body or the “type” attribute of a “PartyID” element must be a URN.
- This URN should comply with the recommendations for URN’s given in section 5.2.5 of this CWA.

The identification schemes which appear as the preferred ones for a party⁴² should comply with the recommendations given in chapter 5.3 “Verification Of Identifiers In Registries” of this CWA.

6.2.6 UN/EDIFACT And According Transport Mechanisms

Unique identifiers are well established in UN/EDIFACT messages. A good example is the identification of the trading partners, i.e. the sender and recipient in EDIFACT Interchanges in the “Interchange Header”.

According to ISO 9735 “Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules” the structure of an EDIFACT interchange is:

	Service String Advice	UNA	Conditional
	Interchange Header	UNB	Mandatory
	Functional Group Header	UNG	Conditional
	Message Header	UNH	Mandatory
	User Data Segments		As required
	Message Trailer	UNT	Mandatory
	Functional Group Trailer	UNE	Conditional
	Interchange Trailer	UNZ	Mandatory

The relevant data elements in the Interchange Header UNB are:

S002	INTERCHANGE SENDER	
0004	Sender identification	C 1..35
	Name or coded identification of the recipient of the interchange	
0007	Partner identification code qualifier	C 1..4
	Qualifier referring to the identification code	
0008	Address for reverse routing	C 1..14
S003	INTERCHANGE RECIPIENT	
0010	Recipient Identification	C 1..35

⁴² The ebMS and CPPA specifications allow to specify multiple identifiers for a party. The one appearing as the first in an according XML document is the preferred one.

Name or coded identification of the recipient of the interchange
 0007 Partner identification code qualifier C 1..4
 Qualifier referring to the identification code

According to the “EDIFACT Syntax Version 4, Release 1”⁴³ the qualifier values for the data element 0007 are:

Value Denotation

....
30	ISO/IEC 6523: Organization identification Self explanatory.
....

Example:

value of	0007 Partner identification code qualifier C 1..4	= 30
value of	0010 Recipient Identification C 1..35	= 008501900298

According to the entry “30 ISO/IEC 6523: Organization identification” the first 4 digits represent an International Code Designator (ICD) value.

As described in chapter 6.1.5, the protocols for the transport (over the Internet) specify mandatory fields for the unique identification of sending and receiving systems.

Recommendations:

For both messages and protocols, it is recommended to use identifiers that comply with the recommendations concerning registration criteria of chapter 5.3.2. For data or header fields that are not specified by the context, it is also reasonable to use Uniform Resource Identifiers (URN's) as specified in chapter 5.2.5.

6.2.7 Trustlabels

A trustlabel confers trust on a business entity (organization and/or part thereof) to the verifier of the trustlabel. It is a human readable alphanumeric code. By clicking on the trustlabel the verifier is directed to additional information. On the WWW there are many systems available for affixing trust to a company or a product.

In this section a specific approach is followed. It is based on 5.4.8 “Community Of Resolution Services” i.e. unique identifiers accessing trustworthy registers are used. The following chain of trust is applied:

(ver)	the verifier of the specified business identifier trusts
(TTP)	a Trusted Third Party which accepts/recognises/accredits
(dir)	the register/directory managed by a specific operator containing
(info)	the information specified by a business identifier ID
(ID-owner)	the owner/licensee of a business ID

43 See <http://www.gefeg.com/jswg/cl/v41/40106/cl3.htm>

Trust-labelling as specified in this section is functioning by applying the following steps:

- The ID-owner/licensee tags an electronic document in the standardised form $TTP_i \rightarrow (dir) \rightarrow ID$ to a trustlabel branded by the TTP_i
- By clicking on this trustlabel a verifier (ver) resolves the stipulated chain of trust starting with
 - o (TTP_i) which redirects the verifier to the accepted/recognised/accredited
 - o (dir) registry where he or she finds the information
 - o ($info$) related to the owner's/licensee's affixed trustlabel
- The TTP_i shows its trust links with other TTPs (TTP_{i+1} , TTP_{i+2} ,). If the verifier of a trustlabel does not know TTP_i he or she can use another TTP_{i+1} , TTP_{i+2} , which will redirect the verifier to the correct information related to the trustlabel.

6.2.8 Presentment Of Conformity Assessment Certificates

Presentment of conformity assessment certificates as specified in the title of this section means

- the presentment that a conformity assessment certificate is issued by an accredited conformity assessment body
- and the presentment of acknowledgment between accreditation bodies concerned so that the system is working internationally.

To gauge correctly an entity and make conformity assessments and measurement as part of it reliable has been an issue for industry and commerce parties since the antiquity. Reliable measurement depends on specific procedures, which require high professional abilities in many different fields of science and technology. Thus, multitudes of organizations/companies specializing in specific fields of measurement and assessment of procedures have emerged. In order to promote industry and commerce needs, the legal basis concerning metrology (measurement) has been created in many countries.

Accreditation is considered a "public service" activity in Europe. It can be delegated to a private company. This system of accreditation and conformity assessment is based on enactment by states/countries and it is enhanced by international agreements and/or bylaws of private international associations.

The basic model is:

- Accreditation: An accreditation body assesses a conformity assessment body in terms of meeting the requirements of suitable auditing competences in a specific area.
- Conformity assessment: A conformity assessment body confirms certain characteristics of an entity, object or process, i.e. it certifies e.g. an organization, organizational units or administrative procedure and issues a certificate corresponding to its capabilities.

A conformity assessment body is:

- A certification body (for management systems, products or personnel)
- An inspection body (e.g. for public health)
- Or a laboratory (for testing and calibration)

Examples:

- The accreditation body accredits calibration bodies to calibrate medical instruments.
- The accreditation body accredits companies to issue ISO 9001 certificates for good management procedures.

- The accreditation body accredits an inspection body for the control of industrial hygiene.

A conformity assessment body allocates identifiers to its certificates of conformity. These identifiers are unique within the domain of the conformity assessment body. The conformity assessment body itself needs to be uniquely identified within the domain of the accreditation body which again is uniquely identified worldwide. Out of the concatenation of all the according identifiers and their embedding in a meta-identification scheme (compare 5.2 “Meta-Identification Schemes”) results a unique identifier for a certificate of conformity.

The according data (especially the validity) concerning a specific certificate of conformity may be accessible in an online registry of the responsible conformity assessment body. The “verification” of such a certificate of conformity means to check if the certificate has been issued by an accredited conformity assessment body (and is still valid). Technically, it is the trustworthy lookup of the certificate’s unique identifier in the registry of the conformity assessment body as described in 5.4.8 “Community Of Resolution Services”. This system can also be used for the presentment of the recognition of foreign accreditation bodies and therefore indicate international trust relationships and interoperability between accreditation bodies.

Following the logic introduced in section 5.4.8 “Community Of Resolution Services” this organizational system of accreditation and conformity assessment can be represented technically.

The following *Chain of Trust* has to be established (according to the terminology of section 5.4.8):

- (ver) the verifier of a *certificate* specified by a business identifier trusts
- (TTP) a Trusted Third Party (*accreditation body*) which *accredits*
- (dir) the register/directory managed by a *conformity assessment body* containing
- (info) the *information specified by the certificate* issued to
- (ID-owner) the *owner of the certificate* that is specified by the said business identifier

Thus, any owner of a *certificate* specified by an identifier who wants the related information of the *certificate* to be made visible/checkable has to append the unique identifier of *the certificate* in a standardised form:

related accreditation body (TTP) → (dir) of related conformity assessment body → certificate identifier pointing to the certificate information (info) → the owner of the certificate (ID-owner)

The explanations above are valid if the verifier (ver) trusts the responsible accreditation body (TTP) beforehand. However, in an international environment where the verifier (ver) is located in another country than the owner of the certificate (ID-owner) he (ver) trusts another TTP. Therefore, the trust links between the TTP’s, i.e. the acknowledgments between accreditation bodies need to be presented as well. For the presentment of the acknowledgment between accreditation bodies the following technical requirements apply (compare explanations concerning trust in section 5.4.8):

The accreditation body i (TTP_i) shows its trust links with (i.e. its acknowledgments of) other accreditation bodies (TTP_{i+1} , TTP_{i+2} , ...). If the verifier of a certificate does not know accreditation body i (TTP_i) he or she can use another accreditation body (TTP_{i+1} , TTP_{i+2} , ...) which will redirect the verifier to the correct information related to the certificate.

6.2.9 Usage In Registered Mail And Similar Systems

Electronic mail is a major tool for business activities between organizations, but additional security services are necessary for both identifying the sender / identifier couple and making sure that the e-mail itself is delivered and not altered. In the current context, the unique identification of parties is key, if the mail aims to settle a legal basis between parties. In certain Member States, regulation(s) are already in place on mails transmitted by electronic means providing the unique identification of

the sender and a proof of delivery. A range of Registered E-Mail ("REM") services is already established and their number is set to grow significantly over the next few years. Without the definition of common standards there will be no consistency in the services provided especially in the context of international business relationships between organizations.

Furthermore, lack of standardization might also affect interoperability between REM based systems implemented based on different models, rather than ensuring a consistent form of service across Europe, especially with regard to the form of evidence provided. In order to move towards the general recognition and readability of evidence provided by registered e-mail services, specifications will be carried on to define technical formats, as well as procedures and practices for handling REM, and the ways the electronic signatures are applied to it.

In this respect, electronic signatures of both sender and recipient shall be considered as the key security component for both uniquely identifying parties and protecting the information. But it is to be noted that a simple "electronic signature" would be insufficient to provide the required trust to an information exchange. Therefore, technical specifications assume the usage of at least an Advanced Electronic Signature, with the meaning of article 2(2) of EU Directive 1999/93/EC.

Basic Registered E-Mail services aim to provide users, in addition to the usual tools supplied by ordinary e-mail service providers, with a set of evidences suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non delivery, of retrieval, etc. of e-mails sent/delivered through such service. These include the following functionalities:

- 1) "Store and Forward" (S&F henceforth), where a REM is directly forwarded to the REM Recipient; and
- 2) "Store and Notify" (S&N henceforth) where the REM Recipient is first notified of that a REM Object is stored and is provided with a reference to the location where the REM Object can be downloaded.

In both cases, REM components interact using external interfaces to REM users, and interfaces to other REM implementations. Evidential services are deemed to comply with legal, regulatory or contractual requirements to provide legal validity and enforceability under domestic or international law e.g. unique identification of parties and integrity of object content.

The reference document for this topic is the ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 2: Data Requirements and Formats for Signed Evidences for REM".

In addition to transport services as provided by existing mailing tools, REM systems offer evidence modules related to the submission, transmission (where applicable) and delivery of the REM Object. The REM users are the REM Sender, the REM Recipient and any Third Party that could be, for instance, the user's organization, a judge in case of dispute, or a party nominated by the REM Sender or REM Recipient for receiving evidences on their behalf. The same entity may act as both REM Sender and REM Recipient. In most implementations, the REM Sender must authenticate to a relevant REM-Management Domain (REM-MDs), but the choice of the authentication mechanism is left to the specific REM-MD. The REM Sender has access to the REM-MD services through a User Agent. In some implementations, delivery is subordinated to REM Recipient's explicit acceptance of the new REM Object. To receive REM Objects addressed to him the REM Recipient must authenticate to the relevant REM-MD, but the choice of the authentication mechanism is left to the specific REM-MD.

The process of a REM relaying triggers events, e.g. delivery (or non-delivery) to the recipient. These events are logged with signed "REM-MD Evidence" messages. Clause 5.2.2 of ETSI TS 102 640-2 lists and describes the components of such a REM-MD Evidence. Clause 5.2.2.1.1 and A.1.4/B.1.4 respectively describe the component (or field) "REM-MD Evidence Identifier" which is used to keep track of issued REM-MD Evidence, for possible later retrieval. The specification requires that the value of this field must be a unique identifier in text-format for every REM-MD Evidence within the issuing REM-MD. As the according REM-MD Evidence provider is free as regards

the specific content of this text-field, it is not unreasonable to use a URN - as specified in chapter 5.2.5 of the present document - containing a unique identifier designating the organization responsible for the REM-MD and an "Organization part Identifier" for the specific Evidence message. Such a URN would not only be unique within the REM-MD but also worldwide.

Two REM-MDs might interoperate together via standard interfaces to provide REM Object exchanges. This is generally the case when the REM Sender and the REM Recipient are not in the same domain and therefore use different REM-MD. In this situation, the REM Object will have to be relayed between disparate REM-MDs.

REM Signatures

The unique identification of both senders and receivers relies on an extensive usage of electronic signatures. Clause 6 of the ETSI Technical Specification 102 640-1 V1.1.1 (2008-10) precisely identifies the different types of electronic signatures that may appear within the REM-MD Messages/REM Dispatches, and general rules that govern their presence within one REM-MD Message/REM Dispatch.

Senders MAY sign the original message submitted to the recipient, supporting the signature with their certificates - qualified or not qualified. If a REM-MD Message/REM Dispatch contains REM-MD Evidences, these have to be signed by the REM-MD in charge of generating them. This may be done by individually signing each REM-MD Evidence or by generating an S/MIME signature on all the parts of the REM-MD Message/REM Dispatch.

Electronic signatures MUST be Advanced Electronic Signatures (AdES) as per specifications TS 101 903 (XAdES) [4] or TS 101 733 (CAAdES) [3]. These electronic signatures MAY include a signed property containing the explicit identifier of the Electronic Signature Policy governing the signing and verifying processes. It is recommended, however, that signature policy requirements, or the signature policy identifier, be included in REM Practice Statement. These electronic signatures MUST include a signed property containing the signing time claimed by the REM-MD.

All the REM-MD Evidences carry one or more date and time elements. If the REM-MD signature is known to be valid the REM-MD Evidence signer's time indications may also be trusted. This time should not, however, be used to check signature validity. These electronic signatures MUST include a signed property protecting the signing certificate. Once generated, a signature time-stamp MAY be computed and added to these electronic signatures.

The above mentioned clauses specify requirements for signature applied to REM-MD Evidence objects for the three data formats supported: XML, ASN.1 and PDF applying the common requirements in the context of specific data formats.

For a discussion concerning PKI and X.509 certificates (used within the REM signing process), please see chapters 0 “

PKI” and 6.2.2 “X.509 Public-Key And Attribute Certificates” of this document.

6.3. Legal Considerations

6.3.1 Legal Effect Of Identifiers

Business identifiers are void of any legal effect as such. It is the context in which they are used that might make them produce legal effect. A private identification scheme could be associated with sets of legal terms that are implicitly applicable in a specific business relationship. An identifier issued by a public authority, such as a VAT number has unique value across the board as it is sufficient to identify a business entity in private transactions as well as in transactions with public authorities. Private identification schemes have legal effect within the group of entities that have accepted them as valid. In an EDI context for example, the closed user group of participants will

recognise the numbering scheme used to provide machine identification of the transacting entities. In a PKI context relying parties recognise the identification scheme within their own context, in case of closed user group, or publicly in line with the prevailing conditions spelled out in a certificate policy of the issuer. In such case the issuer should be aligned or should itself be a trusted anchor to ensure trust. Key to the success of an identifier scheme is acceptance by regulators, other members and possibly exchanges and market places, where such identifiers are used. It is likely that such entities are open to a meta-standard for identifying business entities as long as conflicts with existing schemes are avoided.

6.3.2 Liability Of Providers

The possibility of liability of the issuing organizations is an issue that should be addressed as the issuer provides access to the numbering scheme and its subsequent validation to all interested parties. This accessing could either be limited to registered users or be public; allowing for varying levels of liability to be designated according to the risk levels that the issuer is prepared to accept. The issuer should have the technical capability to provide access to and warrant the integrity of the database hosting the identification scheme. Additionally providing access to the validation data is very important too. If service levels are designated either to the general public or through a service level agreement, the issuer should inform the submitting parties as well as parties seeking validation of service lapses and outages. The successful operation of an issuing authority requires that the liability of the issuer be properly capped; therefore an appropriate risk assessment and subsequent insurance scheme are of paramount importance.

While the liability of registration authorities should follow the same general premises as those prevailing in the case of issuers, it features certain elements that set it slightly apart. As such specific risks associated with the function of registration should be identified. The registration function is served by collecting identification documents and duly transcribing the appropriate input in dedicated databases. Subsequently the Registrar should make sure that the request to the issuer is duly placed. A request could concern the issuance of an identifier or a request for change of status such as revocation, suspension etc. In most cases, however the status would be a request to issue and a request to scratch off the registry. Therefore the risk assessment and associated insurance coverage of a registrar should be limited to transcription errors, that in most cases could be human and the loss of documents. Both these risks are well documented as the banking industry has been dealing with them quite successfully. Additionally the vetting requirements and background checks can be assured by allowing registrars to gain access to private and public appropriate databases in order to cross check the validity of organizational data or the personal data of individuals acting on behalf of organizations (such as the database of stolen or lost ID cards).

6.3.3 Governance Issues

It is important to underline the significance of an organizational structure and a governance scheme to host the possible identification scheme. In this respect the following elements would be considered:

- A governing board to ensure adherence to governance principles
- A management board to execute and carry out day to day tasks
- An advisory board to ensure control and adherence to audit principles
- A technical unit to ensure the uptake, maintenance and valuation of technology used
- A market unit to ensure continuity and adherence to the principle of creating value for the organization.

6.3.4 IPR Issues

As the rightful owner of the identification scheme the issuer authority is in charge of the prevailing legal conditions of awarding identifiers. As previously discussed the numbering itself might be devoid of legal significance. This however might not necessarily be the case if the numbering scheme is accompanied with a specific mechanism to issue the identifiers, legal conditions and statements to support the issuance of the scheme, service conditions and the like. In that case the representations made limit the use of the numbering scheme within the group of authorised users only that have accepted the prevailing conditions. Copyright protection can further be afforded to the issuer with regard to any further statements, trademarks, labels etc., that are based on such identification scheme. Additional accreditation conditions to ensure proper usage cannot be ruled out.

6.3.5 Policy Requirements

Setting the stage for interoperable identity management services for business, can further be facilitated should the requirements for the application layer be spelled out in terms of a set of policy requirements. In the context of public key infrastructure, the certification policy requirements have received broad attention and they have been broadly standardised across the board; there is, however, no such attention reserved for other significant aspects of certificate management as validation policy requirements, application policy requirements and the like. These are equally important in a validation based framework that seeks to service application oriented goals. As a follow up for the activity regarding cyber-identity for business purposes standardising the policy requirements for the application layer is a need that can bear fruit in terms of bringing together the apparently disparate requirements of the various types of users and application service providers.

6.4. Conclusions

Goal Of The Workshop On Cyber-Identity:

The goal of the workshop is to treat the issue of the isolation of different business registries and to show ways to overcome this isolation.

The business plan of the workshop stated: *“Several business registries currently in place address the issue of business Cyber-Identity [...] in a non-uniform manner. A significant amount of resources remains untapped, due to incompatible and non-interoperable business registries that mainly operate in isolation within non interoperable application domains.”*

Rationale:

Trust and Security

Although the term “Trust” is often used within discussions about technical security, “Trust” and “Security” are not equivalent. Technical security is only one important component of a trusted eBusiness infrastructure. Unique identification of organizations and parts thereof, as well as its verification in registers is another component of trust. Unique identification requires interoperability between different identification schemes. The simplest and most obvious prerequisite to achieve interoperability is meta-identification.

Findings:

(a) Basis and requirements for interoperability by meta-identification

It is a conclusion of the CEN Workshop on Cyber-Identity that the meta-identification of unique business identifiers has to follow an “IBAN like” setup (see the discussion of IBAN in chapter

4.1.3 “Overview Of Types Of Business Identification Schemes”): This setup consists in a standardised composition of existing schemes. This means that no new identification schemes have to be invented and implemented.

This composition needs a meta-identification scheme that provides maximum flexibility. Uniform Resource Name (URN) meets this requirement. This leads to the specific conclusion that is: The identifiers have to be given together with the identification scheme in the form of the URN notation (i.e. “urn:...”). See chapter 5.2.5 for the according requirements and recommendations.

(b) Verification/validation of unique identifiers

Unique identification of business entities is one side of the problem. The complementary side is verification of the related organization or part thereof. The discussion of hierarchical versus federated systems for verification shows that only the federation approach is feasible. (The term federation denotes standards of operation that allow data sharing of multiple, independent, self-governing providers without affecting their applications. See 5.4.8 “Community Of Resolution Services”.) Federation/community building can be supported by Trusted Third Parties (TTP) to act as intermediaries for Trust. These intermediaries redirect verification/validation requests to the appropriate registry, i.e. information provider. Specifically see 6.2.7 “Trustlabels” and 6.2.8 “Presentment Of Conformity Assessment Certificates” in the use cases chapter. Trust relationships between these TTPs lead to international/cross-sectoral chains of trust. Please note: the provider of a directory and a TTP can be the same organization. A Technical service provider can act on behalf of TTPs which act as intermediaries.

(c) Benefits and Risks

Overcoming the isolation of different business registries is the issue of this CWA on Cyber-Identity. This CWA renders a considerable contribution for improving this topic. The “IBAN like” setup of world-wide unique identification numbers allows registry providers to keep their customer relations untouched. New services being put in place based upon the proposed unique identification numbers will enlarge the usage of all identification numbering schemes.

Thus a win-win situation will result for the registry providers even if they are competitors. National registration schemes (VAT, commercial registry etc.) will be interoperable with each other and with internationally operating schemes.

The proposed chains of Trust can be built up step by step following Federation principles. Wide international consensus is not necessary in order to start. No scheme provider is obligated (forced) to cooperate.

However there is a risk of a low or wrong perception in the market. Therefore, the message of the win-win situation has to be properly promoted.

(d) Governance issues

On the meta-identification and verification level, the main problem is the correct assessment of identification schemes to be meta-identified and of the corresponding registers respectively, i.e. which schemes the trust intermediary acknowledges as trustworthy and to which registers it redirects verification requests to. An intermediary must be able to act autonomously concerning its decision about the outcome of such an assessment. The according criteria for registration are addressed in section 5.3.1.

The section 5.3.2 gives a recommendation: the main criterion is transparent communication of the registration criteria to the verifier/validator of a unique identifier. Thus liability issues can be controlled.

Next Steps:

The following actions have been identified as suitable steps resulting out of the CEN Workshop on Cyber-Identity:

- (a) Simplifying the URN notation of the unique identifier by applying at IANA for ISO/IEC 6523 as a name space.
- (b) Outlining of the roles of registry providers and of the Trust intermediaries (redirection services):
 - Outlining the organizational and legal relationships with respect to registration and directory access.
 - Outlining the main governance issues, e.g. how to keep liability under control
 - Outlining additional potential business cases (see chapter 6 part 3 use cases).

Annex A

(Informative)

Background Information

A.1 PKI

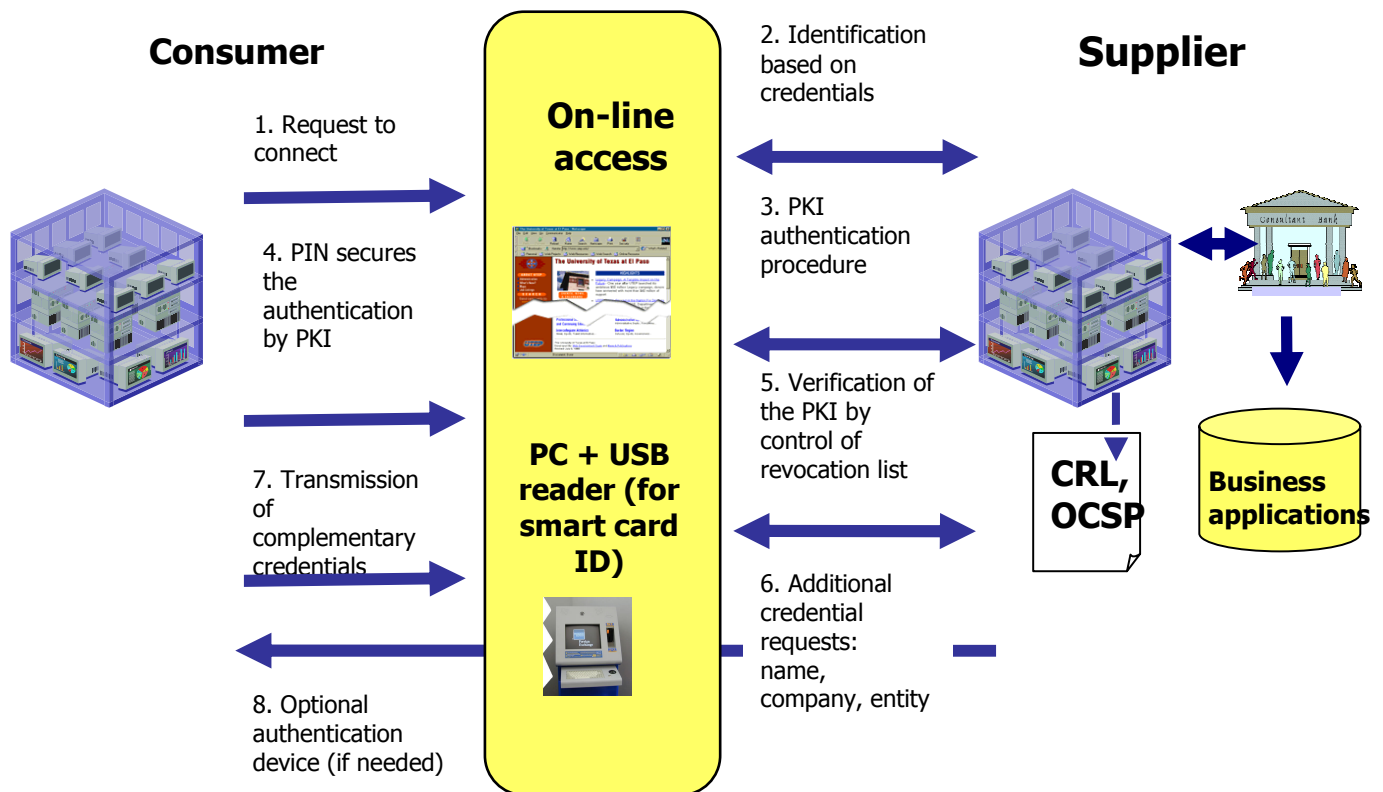
Industry players are yet considering the potential of digital certificates for securely managing the various relationships with their partners. Digital certificates are currently the most powerful way to manage business relationships between business parties on the web. If « identification » only requires a user to submit a credential in the context of a transaction, « authentication » enhances the level of security by requiring the consumer to confirm his ID and his right to access the service.

In this context, the authentication certificate requires a strong registration process prior to connect to a service. In a second step, when the user submits his demand, the server will check his eligibility to connect to the service by controlling his rights on a database and his status from a Revocation list (CRL). For this purpose, each business partner shall precisely define the rules to ensure that the staff entitled to do so securely access the services.

The registration procedure is the first step that allows both consumers and suppliers to enter business relationships. The consumer shall ascertain his ID based on a digital certificate, which confirms his credentials. A Registration Authority issues the digital certificate. For security constraints, it is activated by entering a PIN code that ensures that the right individual uses it.

The authentication shall provide an administrative interface for organizations to define the community of users (and the type of identities that will be accepted) that are to be trusted. For example, organizations can specify the set of userIDs and passwords that are trusted for executing transactions. Similarly, organizations can easily specify — with flexibility and fine-grained controls — the community of digital certificates that are trusted.

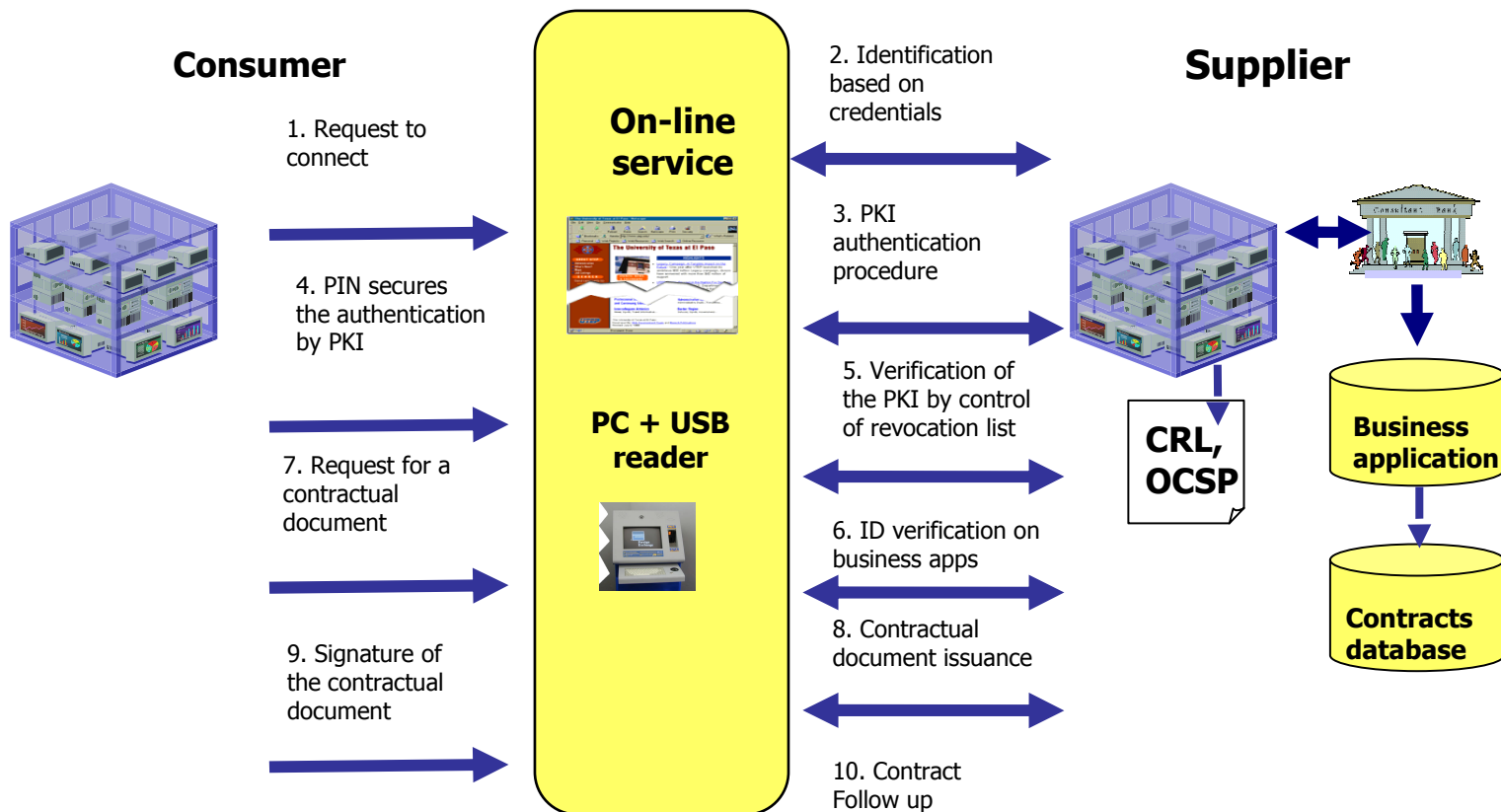
Registration Procedure



Anytime, the consumer connects to the web service, he will enter his PIN code to ascertain that he is allowed to access this specific supplier. The application confirms his rights on the database and the validity of the authentication certificate from a revocation list. Authentication means confirming the ID of the user by a technical device. In the physical world, this is usually done by showing an ID card or passport; on the internet, a digital certificate might confirm – more than a simple log on – that an individual is entitled to claim a specific ID. This is the duty of the issuing procedure to detail the conditions for certificates delivery and operations. Today, qualified certificates can duplicate the physical relationships of individuals in the real world.

Signing a contract or any legal document is a more stringent action than simply connecting and authenticating to an information database. As repudiation is a main issue of the dematerialised world, digital signatures, in addition to authentication signatures, confirm the validity of an action considered as the equivalent of a hand written in the real world.

Signature Procedure



In this case, both parties enter a contractual relationship. Therefore, the consumer shall first authenticate himself based on the procedure described above, then download the legal document for signing, then activate the PIN code that validates his signature. To avoid reputation issues, procedures on both side shall precisely define the rules for the following actions: identification, authentication, signature.

The Verification Service is designed to deliver integrity and accountability capabilities for Web services transactions through centralized digital signatures, time stamping and certificate validation. These services provide critical functions for business-to-business transactions because those transactions typically involve some or all of the following elements:

- Digital signatures to represent approval of the transaction by the organizations involved in the transaction
- Evidence that the transaction occurred at a particular moment in time
- Verification that the transaction has not been altered since it was signed
- And, to deliver auditable records, all of the above must be maintained with the transaction itself for a significant period of time after the transaction occurred

The digital signature capability of the Verification Service provides “organizational signatures” on transactions (rather than the signatures of individuals), a concept which is analogous to the concept of a “corporate seal of approval” on paper transactions.

A.2 eInvoicing

Most of the standardization activities have been carried with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of Value Added Tax, as well as regulations on electronic signatures and EDI.

e-Invoices and digital signatures have been widely addressed in the framework of CWA 15579. eInvoicing implies that an electronic signature is bound to an invoice to ascertain both its transfer and acknowledgment by the addressee. Electronic signature for an electronic invoice can be the signature both of a natural or legal person, as per the applicable law. In case the electronic signature is an electronic signature of a natural person, information should be supplemented that the natural person has acted on behalf of the organization issuing the invoices that should be specified in the certificate. For example, the invoice issuing organization might be specified in the "organization Name".

Where a qualified electronic signature is used, it can only have the purpose of ensuring authenticity and integrity otherwise any member state requiring qualified electronic signatures would be in conflict with the Directive 2001/115/EC provision ("Member States shall not require invoices to be signed"). Where qualified signatures are requested by an applicable legislation, they cannot be given the meaning of commitment to the content of the electronic invoice. Only the purpose of guaranteeing the invoices authenticity and integrity can be assigned to qualified electronic signatures in the domain of eInvoicing. For the purposes of the Directive 2001/115/EC, the term "electronic signature" has the meaning of "electronic seal".

Authentication and integrity have to be guaranteed over the whole storage period of invoices which can be from 5 to 11 years. Electronic invoicing storing systems need to take into account that the electronic invoices have to be stored in a way that the electronic signature stays verifiable over years. If certain information is not available, to ascertain the certificate revocation status at the time of the signature and a time when the signature itself existed, the electronic signature could not be verifiable in the future. Ensuring stored invoices are long term valid, as specified above, depends on both organizational and technical measures. Depending on the trust level of the organization additional technical measures should be applied.

Annex B (Informative) Questionnaire For Issuers Of Unique Identifiers

B.1 Overview

ISO/IEC standard 6523 “Structure for the identification of organizations and organization parts” covers most existing organization identification schemes. However, Unique Identification of business entities is one side of the problem. The reverse side is Verification of the related organization.

The questionnaire published targeted the issuers of unique identifiers and tried to gather information reflecting the procedures used for identifying entities, structures of identification and legal and IPR issues involved.

Initially there was a questionnaire consisting of 40 questions designed, but later on it was decided to limit it down to the most important 13 questions, which were then put on-line. The questionnaire was made available only on-line for a period of one month. Invitations were sent to fill out the questionnaire to all members of the working group, as well as to the European Business Register (EBR) members. EBR is a network of business registers kept by the registration authorities in most of the European countries. For members and other information, see www.ebr.org.

The complete questionnaire, together with the detailed description of the replies, is presented here.

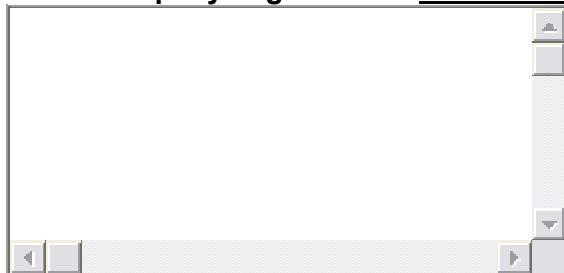
B.2 Questionnaire

Questionnaire for Issuers of Unique Identifiers

00 Personal Data

* **0001: Name** Please write your answer here:

0002: Company/Organization Please write your answer here:



* **0003: e-mail** Please write your answer here:

0004: Web site Please write your answer here:

0005: Country Please write your answer here:

01 Coverage

0101: Is the purpose of registration meant to unambiguously identify an organization?

The term organization may refer to any legal form including a company, subsidiary, single proprietorship, association, governmental body, etc

Please choose *only one* of the following:

☐ Yes

☐ No

02 Scheme structure

0200: What is the name of the identification scheme? Please write your answer here:

0201: Does the identification scheme provide the possibility to identify constituting parts (products, units etc.) within the organization? Please choose *only one* of the following:

☐ Yes

☐ No

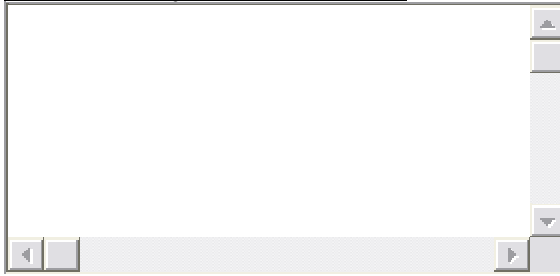
[Only answer this question if you answered 'Yes' to question '0201 ']

02011: If yes, who allocates the organizational part identifier? Please write your answer here:

0202: What is the full format of the identification scheme?

Please describe the length, the meaning of the parts and the layout of the identifier.

Please write your answer here:



03 Procedures

0301: Is the identification scheme dependent on an external register?

A composed identification scheme can be based on a scheme of a third party register.

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

0302: Does the registration authority operate according to procedures that are publicly available?

For example published in publicly available websites

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

[Only answer this question if you answered 'Yes' to question '0302 ']

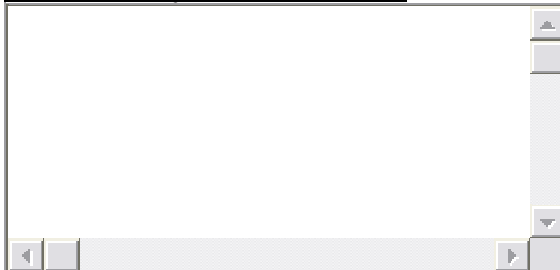
03021: If yes, please indicate the web-address (URL) of these descriptions Please write your answer here:



0303: Please describe (shortly) the allocation/registration procedure for the allocation of an identifier

This includes requirements for the allocation, process of the registration and the like.

Please write your answer here:



0304: What documents do you rely upon or request in support of an application to be included in your registration scheme?

For natural persons this might include passport, driver's licence etc. For legal persons this may include an extract from the Commercial Register, Commercial Courts etc.

Please write your answer here:

0305: Are identifiers that have already been used reassigned after the deletion of entries?

If identifiers are never reassigned, then "No" has to be selected.

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

[Only answer this question if you answered 'Yes' to question '0305 ']

03051: If yes, what is the period of inactivity that is afforded prior to reassigning identifiers?

Please write your answer here:

0306: In your view what are the most common applications that your registration data is used for?

This might include trading partner identification, credit rating, tax purposes etc.

Please write your answer here:

04 Register - Meta Identification

0401: Is the content of your register publicly available in part or whole?

For example register contents could be available on the web

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

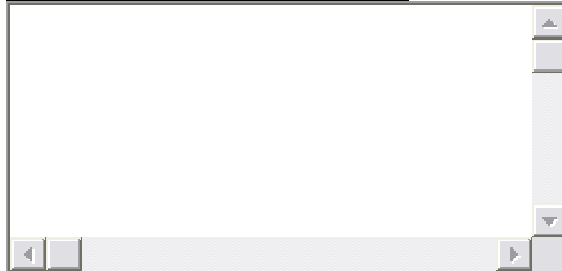
[Only answer this question if you answered 'Yes' to question '0401 ']

04011: If yes, please indicate a web-address (URL) of such a register Please write your answer here:

0402: Which meta-identification schemes are used and recommended for the meta-identification of the identifier-scheme?

Meta-identification is necessary wherever different identification schemes are used within the same context. Examples of meta-identification schemes are Object Identifiers (OID), ISO/IEC-6523 International Code Designators (ICD) or Uniform Resource Names (URN)

Please write your answer here:



05 Legal

0501: Does the use of an identifier have a legal effect within your application context?

Legal effect entails the obligation to use this identifier within a legal / governmental context. Identifiers for governmental use such as VAT and Commercial Register numbers usually produce a legal effect.

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

[Only answer this question if you answered 'Yes' to question '0501 ']

05011: Describe briefly the legal effect of your identifiers and the major applications areas in which they are used.

The description should refer to such application areas as taxation, issuance of certificates, PKI, etc., and their legal effect could include proof of registration, unique identification within a given context, etc.

Please write your answer here:

0502: Does the identified organization own the copyright of its identifier?

Do the Intellectual Property Rights remain the property of the issuer of the identifier?

Please choose **only one** of the following:

- ☐ Yes
- ☐ No

0503: Please describe the restrictions for third parties to use the identifier scheme within their applications and services?

An example for such restrictions is a licence agreement that could lay out the conditions for the scheme in question.

Please write your answer here:

Submit Your Survey.

Thank you for completing this survey..

B.3 Analysis of the replies

There were 21 answers received (17 fully completed and 4 incomplete). The following organizations participated and filled out the questionnaire:

Belgium

- International Federation of Reproduction Rights Organization (IFRPO) (did not complete the survey)

Finland

- National Library
- Finnish Standards Association (SFS)

CWA 16036:2009 (E)

France

- Institut National de la Propriété Industrielle (INPI)

Germany

- Prolist International

Ireland

- Companies Registration Office (did not complete the survey)

Italy

- Actalis SpA

Netherlands

- Netherlands Standardization Institute (NEN)
- Netherlands Chamber of Commerce (KVK)
- SURF foundation

Norway

- Brønnøysund Register Centre

Serbia

- Serbian Business Registers Agency (APR)

Slovenia

- Agency of the Republic of Slovenia for Public Legal Records and Related Services (AJPES)

Sweden

- Swedish companies registration office (Bolagsverket)

Switzerland

- International Standard Audiovisual Number (ISAN)
- Zurich Chamber of Commerce

UK

- Companies House
- Bisnode Limited (did not complete the survey)

Ukraine

- Information Resource Centre (IRC) (did not complete the survey)

International

- GS1
- Odette International

The identities of the companies/organizations answering the questionnaires with the name of the respective identification schemes are as follows:

Company / Organization	Name / e-mail	Web site	Country	Identification Scheme
Serbian Business Registers Agency	Branislav Dobrosavljevic	www.apr.gov.rs	Serbia	Company ID (Serbian: Maticni broj, abbr. MB)
Agency of the Republic of Slovenia for Public Legal Records and Related Services	Tomo Sbrizaj	www.ajpes.si	Slovenia	Matična številka
Brønnøysund Register Centre	Dörthe Koerner	www.brreg.no	Norway	Central Coordinating Register for Legal Entities
ISAN International Agency 30 rue de Saint Jean CH-1203 Geneva Switzerland	Patrick Attallah	www.isan.org	Switzerland	ISAN International Standard Audiovisual Number (ISO 15706)
Odette International Ltd Forbes House Halkin Street London SW1X 7DS	Joerg Walther	www.odette.org		Odette System of Coding And Registration (OSCAR)
The National Library of Finland	Juha Hakala		Finland	ISIL (International Standard Identifier for Libraries and Related Organizations)
NEN Nederlands Standardization Institute	Ton van Bergeijk	www.nen.nl	Netherlands	ASN.1 Object Identifier tree
Companies House	Helen Fletcher	www.companieshouse.gov.uk	UK	Companies Registered Number
The Netherlands Chamber of Commerce	Ricco Dun	www.kvk.nl	Netherlands	Trade Register Number
Bolagsverket/The Swedish Companies Registration Office	Sven Granlund	www.bolagsverket.se	Sweden	Registration Number
GS1	Henri Barthel	www.gs1.org		GTIN
SURFfoundation	Gera Pronk	www.surf.nl	Netherlands	Digital Author Identifier
INPI	Catherine Pagis, Yves Parent	http://www.inpi.fr	France	Siren
PROLIST INTERNATIONAL			Germany	NE 100 (PROLIST)

SFS	Juha Vartiainen	www.sfs.fi	Finland	OID
Actalis S.p.A.	Adriano Santoni	www.actalis.it	Italy	Actalis OIDs
Zurich Chamber of Commerce on behalf of Swiss Chambers	Otto Mueller on behalf of the ZHK chamber	www.zurichcci.ch, www.cci.ch	Switzerland	Swiss Chambers of Commerce Scheme

The following analysis is performed on the 17 fully completed questionnaires that were received.

Coverage Of The Registration

The first question concerned the purpose of registration: is it meant to identify an organization unambiguously or not? Out of the 17 answers received 14 were positive and 3 negative. The negative ones were:

- International standard audiovisual number (ISAN), which is a voluntary numbering system for the identification of audiovisual works. It provides a unique, internationally recognized and permanent reference number for each audiovisual work registered in the ISAN system. The ISAN identifies works, not publications or broadcasts. The ISAN remains the same for an audiovisual work regardless of the various formats in which the work is distributed (e.g. DVD, video recording) or the uses to which it is put.
- Global Trade Item Number, which is the unique GS1 System Identification Number used for trade items (products and services).
- Actalis Object identifiers (OIDs), which are globally unique identifiers used in a number of data objects and protocols including X.509 certificates, Internet protocols, directories, etc.

The second question was on the provision of the identification scheme to identify constituting parts (products, units etc.) within the organization?

Ten of the 14 previous positive replies were also positive. These concerned the schemes of following organizations:

- Agency of the Republic of Slovenia for Public Legal Records and Related Services
- Brønnøysund Register Centre
- Odette International Ltd
- The National Library of Finland
- NEN, Nederlands Standardization Institute
- SURFfoundation
- INPI
- PROLIST INTERNATIONAL
- SFS
- Zurich Chamber of Commerce on behalf of Swiss Chambers

Additionally there was a positive reply from GS1, regarding its GTIN scheme.

Out of the 11 schemes that allowed for identification of constituting parts within the organization, 3 allowed for this identification to be done by the organization itself. These are:

- Odette International Ltd
- SFS
- Zurich Chamber of Commerce on behalf of Swiss Chambers

In another 7 cases the identification of the constituting parts within the organization was done by the assigning organization. These are:

- PROLIST INTERNATIONAL
- INPI
- NEN Nederlands Standardization Institute
- GS1
- The National Library of Finland
- Central Coordinating Register for Legal Entities
- Agency of the Republic of Slovenia for Public Legal Records and Related Services

Structure For The Identification Scheme

The Identification schemes in use follow different layouts (various alphanumerical structures). Here we describe these in detail.

Serbian Business Registers Agency

8 digits: 7 ID digits, 1 control digit

Agency of the Republic of Slovenia for Public Legal Records and Related Services

10 digits: 6 ID digits, 1 control digit (modulo 11), 3 digits part numbers (if organization has more than 999 parts the eighth digit can be a letter)

Brønnøysund Register Centre

9 digits: 8 ID digits, 1 check digit (calculated by weighting the individual digits with standard weights (3, 2, 7, 6, 5, 4, 3 and 2), modulo 11)

Odette International Ltd

ICD (4) 0177 Organization Code (4 an) Organization Part (2 an)

The National Library of Finland

<country code>-<organization code>, e.g. FI-YI (more info at <http://biblstandard.dk/isil/>)

NEN Nederlands Standardization Institute

joint-iso-itu-t(2).country(16).nl(528).nederlandse-organisatie(1)

Companies House (sequential number to all companies on incorporation)

England and Wales: 7 ID digits

Scotland: 6 ID digits prefixed by the initials "SC"

The Netherlands Chamber of Commerce

8 ID digits, e.g. 30123456

Bolagsverket, The Swedish Companies Registration Office

10 digits: 1 digit groupnumber, 5 digits sequencenumber, "-", 3 digits sequencenumber, 1digit checknumber

SURFfoundation

9 digits: Digital Author Identifier (DAI) is a unique national number assigned to every author who has been appointed to a position at a Dutch university or research institute or has some other relevant connection with one of these organizations.

INPI (SIREN number is assigned by INSEE for the creation of the company, or at the declaration of existence of independent workers, artists, authors)

9 digits (depending on activity): Professional / artist author: 000 000 000, Merchant: 000 000 000 RCS, Artisan: 000 000 000 RM 000

SIRET (identifies geographical establishing of business): 14 digits: SIREN (9 digits) + NIC (5 digits). It may therefore be more SIRET from a single SIREN if the company several institutions.

PROLIST INTERNATIONAL

I don't understand the question (to be corrected)

SFS

OID-identifies based on ISO/IEC 8824-1 2002.

In Finland this means a string of numbers of the form:

1.2.246.[identifier of the organization].[organization part]

Zurich Chamber of Commerce on behalf of Swiss Chambers

18 digits: 9 digits organization ID (mandatory – first 3 char. may indicate a registration office), 6 digits organization part, OPI (optional), 1 digit source indicator, OPIS (optional), 2 digits check digits (optional – modulo 97 on used characters)

Only in four cases is the identification scheme dependent on an external register. These are:

- NEN Nederlands Standardization Institute
- Bolagsverket/The Swedish Companies Registration Office
- SURFfoundation
- SFS

Issuing Procedures

In most of the cases the registration procedures are publicly available through the Issuing Organization website.

Serbian Business Registers Agency

www.apr.gov.rs (particular registers, "Laws and regulations", "Electronic data", etc. - fully documented)

Agency of the Republic of Slovenia for Public Legal Records and Related Services

<http://www.ajpes.si>

Brønnøysund Register Centre

www.brreg.no

ISAN International Agency

www.isan.org

Odette International Ltd

www.odette.org

The National Library of Finland

<http://biblstandard.dk/isil/>

NEN Nederlands Standardization Institute

<http://asn1.elibel.tm.fr/en/>

Companies House

www.companieshouse.gov.uk

Bolagsverket/The Swedish Companies Registration Office

<https://snr4.bolagsverket.se/snrgate/startIn.do>

GS1

www.gs1.org

SURFfoundation

<http://www.surffoundation.nl/smartsite.dws?id=13837>

INPI

<http://www.insee.fr/fr/default.asp>

SFS

<http://www.jhs-suositukset.fi/suomi/jhs159>

The allocation/registration procedure for the allocation of an identifier differs from issuing organization to issuing organization and is briefly described in the following paragraphs. The necessary documents needed in support of an application to be included in the registration scheme are also appended. The main conclusion for the documentation needed is that the necessary documents are either provided by the registrant or assumed by an existing membership

Serbian Business Registers Agency.

Very simple allocation scheme: As a First step in the Business entity (BE) (registration process, IDN issuing is centralized in SBRA, as follows: Serial (first free 7 digits in the "allocation block", dedicated to this type of BE) + generation of 8th co

Only SIGNED application (available at SBRA site) and Personal ID copy (natural persons) or extract from Business Register (legal persons).

Agency of the Republic of Slovenia for Public Legal Records and Related Services

All organizations must be registered in Slovenian Business Register (SBR). If they register by subscribing in SBR they get the number at the time of subscription, for others they are registered in other registers and they get the number when they are subs

If organization is not subscribed in SBR they must provide document of subscription.

Brønnøysund Register Centre

A limited company sends an application to file its incorporation to the Register of Business Enterprises. Before information about this company is entered into the Register of Business Enterprises this register will forward identifying information to the

All documents the registrar deems necessary. For companies: Protocol of the general meeting or other documents to show that the company exists. Articles of association.

ISAN International Agency

Registrants (i.e. producers, distributors, broadcasters) of audiovisual (moving images with or without sound) content submit to the central ISAN system standardized metadata. If those are unique in the central database, a unique ISAN is delivered. ISAN is

Standardized metadata, like title, year of production, work type (i.e. film, TV series, Sport event, video game etc.), participants (actor, director, anchor, etc...), duration etc...

Odette International Ltd

Validation of the existence of the applicant company. Validation made by Odette International or Odette National Organizations.

Checks are made against official registers of companies.

The National Library of Finland

The national library assigns local identifiers which are extended to ISILs. The national library maintains a registry of assigned ISIL codes. For the time being only libraries have been identified. Libraries themselves apply of the codes.

The fact that a library really exists is not checked since usually the case is obvious.

NEN Nederlands Standardization Institute

Request for OID by Application Form Validation by NEN Assignment new OID by NEN Create new child OID by NEN Validate by higher Registry Authority

Extract from Commercial Register

Companies House

A sequential 7 digit number is allocated to each company when it is registered and an incorporation certificate is issued.

1. Memorandum and Articles 2. Statement of Compliance 3. Statement of first officers, secretaries and shareholders

The Netherlands Chamber of Commerce

Allocation is part of the automated process of registering an organization

Natural person: ID, Legal person: notary deed

Bolagsverket/The Swedish Companies Registration Office

The company gets a unique registration number when the registration takes place. The number is the next free number in the sequence of numbers

Documents needed are a signed application from the company

GS1

Organizations register with GS1 and get a so-called company prefix, which is a numbering capacity enabling them to identify items

Documents needed depend on the country.

INPI

The Siren is automatically provided by INSEE during the registration, after the registration by the clerk's office.

The documents required are in the Commercial code, which requires for example:

For the natural persons:

- Birth certificate and identity card
- For the foreigners, the foreign trader's permit and the copy of the residence permit
- Matrimonial situation or marriage contract or cancellation of the marriage, divorce or death certificate
- Certificate on the honour of absence of judgment or sanction
- Regulated activities: copy provisional or final authorization diploma or title

For the legal persons:

- Identification of the company: copy receipt of deposit of the deeds of partnership
- Certificate of publication in a legal newspaper of advertisement (JAL)
- For the director, an extract of the act of registration less than three months; birth certificate and identity card; for the foreign, the foreign trader's permit
- For the legal person, an extract of the commercial register less than three months or a justifying title of its existence

PROLIST INTERNATIONAL

I don't understand the question – to be corrected

SFS

Mainly communication by email. Basically any organization can apply.

Actalis S.p.A.

There is a person charged with allocation of a new OID whenever the need arises. That person arranges the OIDs in a hierarchical way based on common sense criteria. The procedure is documented in an internal Actalis document.

Zurich Chamber of Commerce on behalf of Swiss Chambers

Swissfirms SA (owned by the chambers) uses the scheme to allocate IDs to the customers in a yellow page directory; it is also used in a Swissfirms Label to redirect a verifier to the entry in the Swissfirms Database

The documents needed are assumed from membership at a Swiss Chamber of Commerce.

In the majority of the cases (15/17) identifiers that have already been used are not reassigned after the deletion of entries. Only in the case of Actalis S.p.A. are they reused.

Applications Areas

The application areas for which the registration data is put in use have to do with basic business entity identification in various areas. The most common are:

- State use
 - Tax authority
 - Statistics
 - Pension funds
 - Health informatics
- Bank use
- Commercial use
 - Trade partners identification/information
 - Audiovisual content
 - RFID
 - Libraries

In the majority of the cases, with the exception of the Netherlands Standardization Institute (NEN), the content of the register is publicly available from the respective organization website.

Meta-Identification

As for meta-identification schemes used or recommended for the meta-identification of the identifier-scheme, there is mixed feeling. Many organizations (8) do not use any meta-identification scheme or see no need for it. For the ones seeing usage in this area the answers were using the OID based on ISO/IEC 6523 or ISO/IEC 15459 (2), or the Company name and number (1), or an OID (1).

Legal/IPR Issues

In 10 out of the 17 replies the identifier has a legal effect, usually having to do with unique identification within the public sector, tax authorities, social security and banking or with the identifier having to be provided with all company documents related to the Register of Commerce and Trade. This identifier is available in all databases related with these topics and is very widely spread for all online and offline applications. The company number has to appear on all business stationery. Incorporation also allows a company to exercise its business activities, borrow money etc.

In the specific case of Actalis, certain identifiers have a legal effect, because they attest the compliance of the corresponding Actalis' PKI policies to the Italian digital signature legislation and rules.

In most of the cases the company does not own the copyright to the identifier itself, which is held by the Issuing Organization. Finally the Issuing Organization usually does not pose any restrictions on the usage of the identifier.

Annex C (Normative) Summary Of Recommendations

5.2 Meta-Identification Schemes:

5.2.5 Requirements And Recommendations:

Considering the explanations above, the following recommendations can be given for the insertion of unique business identifiers in electronic documents (the focus is on machine-readable documents):

- The identifier has to be given together with the identification scheme in the form of the URN notation (i.e. “urn:...”) if the context or document format does not define the usage of a specific identifier scheme (e.g. the GS1 EANCOM® profile for UN/EDIFACT messages mandates the usage of a GLN for the identification of locations).
- If possible, a business identifier shall be embedded in the URN under a registered formal namespace identifier. (See <http://www.iana.org/assignments/urn-namespaces/> for a list of registered URN namespace identifiers.)
- If a registered ICD value according to ISO/IEC 6523 exists for the identification scheme, the business identifier shall be meta-identified with this ICD value.
 - In case that the business identifier is purely numeric (consisting of digits 0 to 9), the identifier should be embedded in a URN as an OID.
Example: urn:oid:1.3.2.552120784 denotes the SIREN (official French company identifier) 552120784. The ICD value of the SIRENE/SIREN system is 0002, which shows up in the URN as the trailing “2” of the OID “1.3.2”.
 - Otherwise, the identifier may be embedded in a URN under the namespace “urn:oasis:names:tc:ebxml-cppa:partyid-type:iso6523”
Example: In
urn:oasis:names:tc:ebxml-cppa:partyid-type:iso6523:0169:CH-020.3.030.308-0 denotes the Swiss Commercial Register Number CH-020.3.030.308-0. The ICD value for Swiss Commercial Register Numbers is 0169.
 - The workshop will apply for the registration of a URN namespace for iso6523 at IANA. The according procedures will be assessed and ISO/IEC JTC 1, “Information technology”, Subcommittee SC 32, “Data management services” (responsible for the ISO/IEC 6523 standard) will be contacted.
The reason for this step is that the URN shown in the previous bullet is rather lengthy. A URN of the type “urn:iso6523: 0169:CH-020.3.030.308-0” is easier to handle.

Concerning the mapping of unique business identifiers, the following recommendation can be given:

- An organization should publish a URL that points to a document which lists the relevant identifiers that identify this organization. It is recommended that this URL contains the according identifiers as URN's.

An Issuing Organization or registration authority must have a documented and publicly available policy for registration, renewal and updates (concerning the organization and all registered attributes). This policy must address the topics described in 5.3.1 “Registration Criteria”.

5.3 Verification Of Identifiers In Registries

5.3.1 Registration Criteria

The reliability of the information designated by an identifier depends mainly on the quality of the registration. This means that it has to be transparent to a relying party how the information about an entity in a register is verified by the registrar. Therefore, operational procedures are a key factor of organizational registration. For a systematic approach of the topic see ISO/IEC 6523-2 "Registration of organization identification schemes". The considered criteria for the evaluation of operational procedures are:

(c) Criteria for Issuing Organizations allocating identifiers to business entities, i.e. for identification schemes of organizations and parts thereof

(d) Criteria for meta-identifier registration of such identification schemes

Criteria for meta-identifier registration rely on the criteria for current identification schemes according to (a). The authority which issues meta-identifiers according to (b) relies on the documented and approved criteria for identifier allocation by Issuing Organizations.

(a) Criteria for identification schemes of organizations and parts thereof

- Strength of the initial registration of the organization to be registered: the procedures contain registration rules for
 - Existence of an organization:
 - High: audited entry in an official registry, e.g. commercial registry, VAT registry, private or third party registry with vetting requirements in place etc.
 - Medium: presenting (sending copies of) receipts of phone bills etc.
 - Low: self-declaration, phone book entries
 - Responsible natural persons acting on behalf of the registered organization:
 - High: face-to-face registration (presenting official documents and signing of registration documents)
 - Medium: presenting (sending copies of) personalised documents, receipts of phone bills etc.
 - Low: un-audited self-declaration
 - Any registered attributes (e.g. ISO 9001 compliance, turnover values etc.):
 - High: Audit by an (accredited) third party
 - Low: un-audited self-declaration
- Renewal of registration:
 - High: periodic face-to-face renewal, re-auditing of registered attributes etc.
 - Medium: proof by paying periodic registration fees
 - Low: none
- Updates/changes of registered data:
 - High: contractual obligation of the registered entity to communicate any changes of its registered data
 - Low: none
- Publication of criteria:
 - A practice statement of applied criteria has to be available.

(b) Criteria for meta-identifier registration

In the context of this document only two criteria are relevant:

- Public statement of the responsibility of the registration authority for meta-identifiers
- Publication of the allocated meta-identifiers with a reference to the related criteria applied by the Issuing Organization

5.3.2 Recommendations

An Issuing Organization or registration authority must have a documented and publicly available policy for registration, renewal and updates (concerning the organization and all registered attributes). This policy must address the topics described in 5.3.1 "Registration Criteria".

5.4 Resolution Interfaces/Protocols And Services:

5.4.10 Requirements And Recommendations

The following is recommended for providers of resolution services for unique identifiers:

- Register interfaces must be available over HTTP. These interfaces may also be available over HTTPS. (Please note that this does not preclude the parallel support of other protocols for resolution.)
- It must be possible to make a query over HTTP with an identifier as input.
- Queries for identifiers should be possible with the HTTP GET method (in accordance with chapter 9 "Method Definitions" of IETF RFC 2616)
- A register provider must offer an interface in HTML/XHTML.
- It is recommended that register providers offer a machine-readable interface in the XML-format. (Please note that this does not preclude the parallel support of other formats.)
- A register service provider must publish an OpenSearch description file that specifies the URL's for identifier-queries over HTTP and/or HTTPS. The description must contain a URL for an HTML-interface. If additional interfaces are available, the description must contain the according URL's as well.
Please consider chapter 6.1.8 for more information about OpenSearch.
- It is recommended that registers publish at least minimal information (such as an organization's name) free of charge.

The following is recommended for providers of resolution services for unique identifiers:

- Register interfaces must be available over HTTP. These interfaces may also be available over HTTPS. (Please note that this does not preclude the parallel support of other protocols for resolution.)
- It must be possible to make a query over HTTP with an identifier as input.
- Queries for identifiers should be possible with the HTTP GET method (in accordance with chapter 9 "Method Definitions" of IETF RFC 2616)
- A register provider must offer an interface in HTML/XHTML.
- It is recommended that register providers offer a machine-readable interface in the XML-format. (Please note that this does not preclude the parallel support of other formats.)
- A register service provider must publish an OpenSearch description file that specifies the URL's for identifier-queries over HTTP and/or HTTPS. The description must contain a URL for

an HTML-interface. If additional interfaces are available, the description must contain the according URL's as well.

Please consider chapter 6.1.8 for more information about OpenSearch.

- It is recommended that registers publish at least minimal information (such as an organization's name) free of charge.

The following is recommended for providers of resolution services for unique identifiers:

- Register interfaces must be available over HTTP. These interfaces may also be available over HTTPS. (Please note that this does not preclude the parallel support of other protocols for resolution.)
- It must be possible to make a query over HTTP with an identifier as input.
- Queries for identifiers should be possible with the HTTP GET method (in accordance with chapter 9 "Method Definitions" of IETF RFC 2616)
- A register provider must offer an interface in HTML/XHTML.
- It is recommended that register providers offer a machine-readable interface in the XML-format. (Please note that this does not preclude the parallel support of other formats.)
- A register service provider must publish an OpenSearch description file that specifies the URL's for identifier-queries over HTTP and/or HTTPS. The description must contain a URL for an HTML-interface. If additional interfaces are available, the description must contain the according URL's as well.
Please consider chapter 6.1.8 for more information about OpenSearch.
- It is recommended that registers publish at least minimal information (such as an organization's name) free of charge.

6.2.4 UBL

Recommendations

- A UBL community should specify a list of allowed identification schemes to be used in the "EndpointID" and "PartyIdentification ID". This list must include the relevant indications of meta-identification in the "schemeID" attribute.

6.2.5 ebXML Messages / ebXML CPPA

Recommendations

- The URI to be included in the body or the "type" attribute of a "PartyID" element must be a URN.
- This URN should comply with the recommendations for URN's given in section 5.2.5 of this CWA.

The identification schemes which appear as the preferred ones for a party should comply with the recommendations given in chapter 5.3 "Verification Of Identifiers In Registries" of this CWA.

6.2.6 UN/EDIFACT And According Transport Mechanisms

Recommendations:

For both messages and protocols, it is recommended to use identifiers that comply with the recommendations concerning registration criteria of chapter 5.3.2. For data or header fields that

are not specified by the context, it is also reasonable to use Uniform Resource Identifiers (URN's) as specified in chapter 5.2.5.