CEN

WORKSHOP

AGREEMENT

CWA 16036

November 2009

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

Ref. No.:CWA 16036:2009 D/E/F

Contents

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

Bestelformulier

Stuur naar:

NEN Standards Products & Services
t.a.v. afdeling Klantenservice
Antwoordnummer 10214
2600 WB Delft

NEN Standards Products & Services

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T (015) 2 690 390
F (015) 2 690 271

www.nen.nl/normshop

Ja, ik bestel

__ ex. CWA 16036:2009 en Cyber-Identity - Unique Identification Systems For Organizations and Parts Thereof € 53.00

Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. www.nen.nl/nieuwsbrieven

Gegevens

Bedrijf / Instelling

T.a.v. O M O V

E-mail

Klantnummer NEN

Uw ordernummer BTW nummer

Postbus / Adres

Postcode Plaats

Telefoon Fax

Factuuradres (indien dit afwijkt van bovenstaand adres)

Postbus / Adres

Postcode Plaats

Datum Handtekening

Retourneren

Fax: 015 2 690 271
E-mail: klantenservice@nen.nl
Post: NEN Standards Products & Services,
t.a.v. afdeling Klantenservice
Antwoordnummer 10214,
2600 WB Delft
(geen postzegel nodig).

Voorwaarden

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typefouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.