Summary of CEN Workshop Agreement (CWA) 16036 on Cyber-Identity: Unique Identification Systems For Organizations And Parts Thereof

By Adrian Mueller (appointed expert by CEN) and Dr. Otto Mueller (WS member)

This document is a summary of the CEN CWA 16036:2009. The CWA 16036:2009 can be downloaded from the CEN FTP-server:
ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/CWA16036CyberID.pdf

Abstract: Unique identifiers of organizations (and parts thereof) point to information related to the organization (or to a part thereof). They are provided by registration authorities like GS1, D&B or official Commercial Registries which in turn are qualified by meta-identifiers. Applying and verifying such addressed information opens up a new range of applications in areas like eCommerce, Supply chain, eInvoicing, conformity assessment or using such logical identifiers as a reliable routing and addressing scheme.

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)

1   Introduction and Scope

In electronic communications, to gain the trust and confidence of transacting parties, a required element is certainty regarding the organizations involved. 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.

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 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 document concentrates on the usage of unique identifiers in "open" systems and user groups. Stress is laid on identifiers used in open exchange and which can be verified in directories accessible over the Internet. 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), 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.

2 Overview Of Types Of Business Identification Schemes

Broadly, registration bodies can be divided in three models:

A centralised model: 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). The information is held in a centralised directory.

A decentralised model: 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.)

Examples of business identification schemes (see specifications in CWA 16036:2009):

- Global Location Number GLN (by GS1 to identify legal entities, trading parties and locations
- SIRENE the French national numbering system for communication with the French government for administrative issues.
- Bank Identifier Code BIC or SWIFT code to identify financial institutions world-wide
- ODETTE code for identifying business entities in the European automotive industry

- Data Universal Numbering System D-U-N-S to define corporate firms starting from headquarters and integrating subsidiaries and foreign branches
- CREFO number to facilitate the assessment of creditworthiness of companies (Germany, Austria, Switzerland)
- Easynumber by COFACE company for searching and uniquely identifying companies throughout the world
- International Bank Account Number IBAN (by BIC identified bank to identify a specific account)

3   Applications And Associated Requirements

3.1   Application areas:

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. The application area ranges from eCommerce to Supply chain, eInvoicing or relying on certificates issued by conformity assessment bodies and others.

The focus is always interoperability of applications: Interoperability in eBusiness and eGovernment does not only concern agreed technical formats of documents and protocols among (trading) parties (syntactic interoperability), common vocabularies 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 requirements are meta-identification and access to trustworthy registers. Therefore the topics treated in detail in the CWA are:

3.2   Meta identification schemes:

A numbering system that forms an umbrella over existing systems by assigning identifiers to identification schemes. Three specific meta-identification schemes[1] have been identified as meeting the (governmental and business) requirements in terms of persistence, standardisation capabilities, proper documentation and applicability.

3.2.1   Recommendation

The recommendation for the umbrella numbering system is using an "**IBAN like" approach** following the Uniform Resource Names (URN) approach.

3.3   Verification of identifiers in Registries / Resolution interfaces/protocols and services:

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. The recommendations are: 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).

---

[1]   International Code Designators ICD ISO/IEC 6523-2; Object Identifiers OID according to ISO/IEC 9834-1; Uniform Resource Names URN according to RFC 2141 And 2396

3.3.1 Interfaces and Protocols

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. This raises the question about which protocol-standards should be mandated or recommended. Different protocols[2] are compared and discussed with respect to security, deployment, presentation, flexibility and performance.

3.3.2 Community of resolution services:

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

In order to achieve interoperability of unique business identifiers 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. A harmonised, federated system of resolution services depends on agreed standards for meta-identification.

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. 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).

3.3.3 Requirements and recommendations:

Detailed requirements and recommendations are given concerning register interfaces and protocols. The main recommendations are: Register availability over HTTP and HTML/XHTML interface. It is also recommended that registers publish at least minimal information (such as an organization's name) free of charge.

4 Use Cases And Specific Issues

4.1 Technologies In Use

4.1.1 Unique identification

Some technologies which support means for unique identification are discussed:

Uniform Resource Identifier concept - URI: The 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

---

[2]   Domain Name System (DNS) Based Systems; Hypertext Transfer Protocol (Secure) - HTTP(S);
        Lightweight Directory Access Protocol (Secure) - LDAP(S); SOAP and ebXML Messaging Services (ebMS)

extendable number of protocols, existing, invented for the web itself, or to be invented in the future. URIs, which refer to objects accessed with existing protocols like HTTP are known as "Uniform Resource Locators" (URLs).

Internationalized Resource Identifiers – IRIs: 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).

OpenSearch: OpenSearch stands for a collection of simple XML-based formats for the sharing of search results. 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, e.g. with a unique business identifier as input.

4.1.2 Relying technologies

Some technologies are discussed that 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:

Public Key Infrastructures – PKIs: PKIs are targeting on closed or open user groups. Mainly for the open user groups the receiver of a certificate faces the problem to identify an organization or its part within a certificate. In this context unique business identifiers for organizations and parts are considered. They should be persistent over time and be verifiable in trusted data bases.

UN Electronic Data Interchange For Administration, Commerce, and Transport UN/EDIDFACT: Concerning the exchange of messages according to UN/EDIFACT (United Nations Electronic Data Interchange For Administration, Commerce, and Transport) the following two aspects regarding unique business identifiers have to be considered separately: The usage of identifiers in the messages themselves and their usage for the transport in open networks, including the routing of these UN/EDIFACT messages. For the latter meta-identification of unique identifiers of organizations and parts thereof is relevant. New protocols describe the fields for sender and recipients of messages.

Universal Business Language - UBL: 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 relating to business data.

Electronic business using eXtensible Markup Language - ebXML: 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. Within this context the format of the "PartyID" element and how unique business identifiers have to be included in it is of great relevance; also for its verification in a trusted database.

4.2 Use cases

The former chapter "Technologies In Use" shows the issues and questions that arise concerning the application of unique business identification within these technologies. This chapter "Use Cases" is dedicated to how the issues can be solved. The following Use Cases are a selection of significant and promising examples which demonstrate that the findings of chapter "Applications And Associated Requirements" can be used in different important application areas; i.e. well known application fields but also new applications benefiting from harmonised unique business identification like "Trustlabel" and "Presentment Of Conformity Assessment Certificates".

Summary CWA 16036:2009

4.2.1   X.509 Public-Key And Attribute Certificates

Two specific examples of inclusion of identifiers of organization are shown:

Extended Validation" (EV) SSL Certificates: The "Guidelines for the issuance and management of Extended Validation Certificates"[3] of the CA/Browser Forum apply. Their goal is to reach a higher level of trust for EV SSL Certificates than for traditional SSL/TLS (Secure Socket Layer/Transport Layer Security) certificates. The EV SSL guidelines require that a Registration Number is included in "Subject Distinguished Name" of the certificate.

French Governmental General Security Framework: In a specific Domain Name component a unique identifier of the organisation an employee belongs to is included by using meta-identification.

4.2.2   eInvoicing

The CWA 15576 "Recommendation to allow coded identifiers as an alternative to the current unstructured clear text identifications"[4] is discussed. The topic is the established practice in (automated) eInvoicing (and eProcurement in general) that the trading parties – of course including the taxable person – are represented by unique identifiers.

4.2.3   Universal Business Language - UBL

The UBL specification contain 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. A UBL community should specify a list of allowed identification schemes to be used in the "EndpointID" and "PartyIdentification ID".

4.2.4   ebXML Messages / ebXML Collaborative Partner Profile Agreements CPPA

The specification demand the usage of the "PartyID" element for the unique identification of business parties with a Uniform Resource Identifier (URI) as (meta-) identifier; for which specific recommendations are given.

4.2.5   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". Recommendations are given for data and header fields.

4.2.6   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 CWA trust-labelling is functioning by using a tier structure. The verifier of a trustlabel relies on a specific Trusted Third Party which redirects the request of the verifier to a directory containing the information concerning the trustlabel. Such Trusted Third Parties are organised in a federated system based on agreed meta-identification. It is not a centralised system.

4.2.7   Presentment Of Conformity Assessment Certificates (Accreditation)

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 Presentment of conformity assessment certificates is based on a

---

3   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.evcert.

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

tier structure like the Trust label system. A certificate is issued by a conformity assessment body which in turn is accredited by an accreditation body. An accreditation body is usually a governmental agency which is internationally federated with other accreditation bodies.

4.2.8   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. 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. New standards for REM services and the use of identifiers are referenced.

4.3   Legal considerations

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. Based on this statement the following topics are analysed:

- Legal effect of identifiers
- Liability of providers (of identifiers)
- Governance issues
- IPR (Intellectual Property Rights) issues
- Policy requirements

4.4   Conclusions

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. It is a conclusion that the meta-identification of unique business identifiers has to follow an "IBAN like" setup which consists in a standardised composition of existing schemes. This composition needs a meta-identification scheme that provides maximum flexibility. Uniform Resource Name (URN) meets this requirement.

The complementary side of unique identification 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. Federation/community building can be supported by Trusted Third Parties (TTP) to act as intermediaries for Trust.

➢ 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.