Open Source Solutions for Interoperability in the eID Domain

Bud P. Bruegger <bud@comune.grosseto.it>, OpenPortalGuard Project and Town of Grosseto (Italy)
Jan van Arkel <arkel@cardlife.nl>, Ambassador CEN/ISSS WS eAuthentication (The Netherlands)
Stef Hoeben <Hoeben.S@zetes.com>, OpenSC Project and Zetes PASS (Belgium)
Antonino Iacono <ant_iacono@tin.it>, OpenSignature Project (Italy)

Problem Statement

Europe has now 25 countries and over 450 million citizens. The increased mobility of citizens who travel both within Europe and worldwide, increases the importance of the remote electronic delivery of services in all sectors ranging from e-government, over e-health, to e-business and e-procurement. Mobile citizens will typically need to access services in their home country while away and services in the places where they conduct business or acquire properties. Remote service delivery is a key to the efficiency of administration and promises major cost savings by avoiding unnecessary travel.

For remote services to substitute the personal presence of citizens at government counters or office desks, a very high level of security is required. Typically, these services deliver personal and at times sensitive data and/or involve legally binding transactions. It is therefore imperative that the service provider has certainty about the identity of the user and has means of proof that given declarations or requests were issued by a given person. In other words, remote services require secure means of *identification*, *authentication*, and *digital signature*. Identification provides data describing the user; authentication verifies that a valid token is used by its legitimate owner and links the token to the person's identifying information; digital signature provides the means to prove that a given transaction was issued by that person.

In order to support Europe- and world-wide mobility, **interoperability** of technical solutions to the problems is of utmost importance. Citizens will typically interact with service providers from multiple countries and operate from both home and abroad. The typically nationally issued tokens (or eID cards) that citizens use to identify themselves electronically need to be accepted by all service providers Europe wide and the client software installed in public offices needs to accept all cards. Or in more detail, full interoperability implies the following requirements:

- server-side provisioning systems must be able to extract and verify identity information from all eID cards in order to build personal user profiles that grant rights for the access to certain services
- server-side access control systems must be able to authenticate users no matter which eID card they use. In some cases, for example for citizens with residence abroad, users may own more than one token and servers need to identify them independently of the token used.
- Client-side middleware, at least that installed in public offices and access points, must support the basic functionality of identification, authentication, and digital signature with any of the possible eID cards.

Considering the large variety of possible platforms (Windows/Intel, Linux and BSD variants on various CPUs, proprietary Unices, PDAs, smartphones, and potentially embedded devices) used to access remote services, all solutions should be multi-platform in order to bring full benefits.

The Vision Document of the CEN/ISSS WS eAuthentication [http://www.cenorm.org/CENORM/BusinessDomains/businessdomains/isss/activity/eauthstrategicvision.pdf] provides a more extensive discussion of the problem domain.

This paper takes a medium term perspective, focusing on solutions that provide interoperability in the current situation of high diversity. It supports a seamless transition to a possible longer term solutions that increases homogeneity and could result from a large-scale coordination and standardization effort. The discussion focuses on services delivered over the Web (HTTP, HTML) and tokens implemented as smartcards. To respect national autonomy, card issuance and management issues are excluded from the scope.

Current Situation and Solutions already in place

The need for electronic identity management is generally recognized by all European governments and there is a consensus that smart cards (eID cards), PKI, and biometrics are the solution to the problem. The introduction of eID cards is a priority in the eGovernment strategy of several European countries and the Resolution of the future Information Society policy of the Union, adopted on 10 December 2004 by the Council of the European Union, identifies the following as one of six priorities [http://europa.eu.int/ida/en/document/3652/194]:

> *To create a favourable environment for industry and the public sector to develop, both **in Europe and globally**, effective and **interoperable** solutions, in particular for electronic payments, **authentication, identity management** as well as security.*

The following pieces of regulation and standardization at European level have provided guidance to national initiatives: Privacy Directive, E-Sign Directive, CEN CWA 14890. Further, IDA's Bridge CA [http://europa.eu.int/ida/en/document/2318] covers an important role in the infrastructure domain.

Most of this guidance addresses the area of *digital signature*, however; much less support is available in the area of *identification* and *authentication*. For example, it is not clear yet whether the E-Sign Directive is applicable to identification and authentication or whether specific regulation is needed. Also, technical standards like CEN/ISSS WS eAuthentication [http://www.cenorm.org/CENORM/BusinessDomains/businessdomains/isss/activity/e-auth_external_enquiry_for_cwas.asp] are only now emerging and have yet to be implemented. It is therefore not surprising that in regard of identification and authentication, existing eID initiatives are typically of a predominantly national character [http://www.cenorm.org/CENORM/BusinessDomains/businessdomains/isss/activity/eauthstrategicvision.pdf].

In the domain of electronic passports, standardization by ICAO and the European Council[1] promises a high level of homogeneity and interoperability. In the domain of eID cards, while there have been several efforts of international coordination such as the Porvoo Group and the Global Collaboration Forum (EU, U.S., Japan, Global Platform), these have concentrated on a loose exchange of information and experience, rather than on the implementation of a common, globally interoperable solution. The need for a more comprehensive orchestration of national efforts has only been recognized recently in the first meeting of the World eID Steering Committee (Prague, December 2004). It is not yet clear whether this effort will be successful and in what times it can bear fruits.

1 EU concil regulation on ePassports 15152/04 of December 10 2004 offering more security and mandating the inclusioin of biometrics in the passports (facial in 18 months, fingerprint in 36 months)

Analysis of Shortcomings

In the current situation, several European countries issue or plan to issue eID cards [http://www.cenorm.org/CENORM/BusinessDomains/businessdomains/isss/activity/eauthstrategicvision.pdf]. The absence of tight coordination has resulted in a very high degree of diversity; national solutions differ largely in the type of cards used (APDUs), the file system layout, the kind of data included in certificates and data files, the kind of ID (Common Name) used for the card/card holder, and even the functionality provided (e.g., not all cards support digital signature). Similarly, software solutions strictly have only a national or even sub-national (support for a subset of national cards) scope; they usually work only with the eID card(s) of a single nation.

Not surprisingly, interoperability of these national solutions is extremely poor (see for example, eEpoch: http://www.nestor.uniroma2.it/porvoo6/doc/Theo_Van_Sprundel_eepoch rome .pdf, SPES: http://www.spesproject.org/). While the fact that the number of issued cards is relatively low compared to the population may suggest the possibility of rapid change, it is important to be aware of the significant investment that many countries have already made in their solutions: finding consensus among all stakeholders, the creation of an eGovernment strategy and the necessary legal bases, and the design and implementation of the national card issuing and maintenance infrastructure has often taken years before the first card was even issued. Together with the fact that cards are valid for typically five years, this suggests that a high level of diversity will remain characteristic in the medium term.

From this perspective, interoperability in the short and medium term can only be achieved through middleware: a single set of client-side and server-side software must support the whole range of eID cards. In particular, the following software modules and standard interfaces are necessary:

- a client-side smartcard interface module that enables SSL authentication from a web browser (PKCS#11 and/or CSP[2]). Typically, this module detects which eID card is inserted in order to adapt to its characteristics. The functionality of the required module is well specified by the card specifications on one side, and the standardized interface towards the browser on the other. Problems arise solely for the support of eID cards whose specification is not published; this knowledge is a prerequisite for interoperability. Note that for the longer term this issue is addressed in the ISO 24727 standard (under construction) part 2, card edge API.
- a client-side module that renders identity information from the card accessible to remote web applications in support of provisioning. The module adapts to different cards and makes the raw[3] files of a given eID card (certificate and possibly several data files) accessible to the server. It is important to notice the lack of a standardized interface through which remote web applications can access identity data. In the current situation, even for a single eID card, different web applications typically use widely different solutions for accessing the data. These can range from applets over browser plugins to ActiveX objects, most are restricted to a single platform, many only work with Java and/or JavaScript enabled browsers, usually they require solution-specific client-side software installations, and all have widely different APIs (see http://prdownloads.sourceforge.net/opensignature/upi-eng.pdf?download). A standardization of the API that can be used by different web applications is necessary. Explicit user consent has to be guaranteed before providing data to remote servers. Again, the availability of access specifications for various eID cards is a prerequisite. Note that for the longer term this issue is addressed in the ISO 24727 standard (under construction) part 3, Application API.
- A client-side module that supports the digital signature of HTML forms used by remote web applications and possibly the signature and upload of local documents in certain important document formats[4]. The current situation and requirements are very similar to the above module.

2 A CSP to PKCS#11 gateway such as CSP11 can reduce the problem to a single module.

3 The incentive to send raw files is that raw formats are necessary for verification and that client software cannot be trusted to perform this task.

4 The limitation of formats is motivated in the requirement to make explicit to users what they are asked to sign.

Beyond this, security, user awareness and explicit consensus, and a clear and homogeneous user experience across various remote web-applications is of utmost importance. These characteristics have to be guaranteed by an in-depth study. Again, the standardization of an API is necessary.

- A server-side module that requests (using the API of the corresponding client-side module) and, where possible, verifies the identity data contained in eID cards. With many cards, verification is possible through the use of digest information for the various data files. This digest information is either contained in the certificate or signed in some other way. The module is further responsible for parsing the various files and presenting the data in a uniform XML data set that reflects the ICAO logical data structure. A study has to show whether the functionality should always extract the complete set of data or offer different levels of information with increasing detail/sensitivity. For example, it may be often necessary to know the name, date of birth and nationality of a person, but access to biometric facial image data may be justified only in case of border control usage, while the biometric template of a fingerprint should never leave the card but only be used for on-card matching of biometric data. Obviously, this requires precise knowledge on which identity information is managed in which form on various eID tokens and what mechanisms of verification are applicable.
- A standard interface is needed to guide the implementation of a site-dependent[5] module that maps the identity data to a Principal ID that is used as identifier for the person in the domain of the site. The corresponding module is used to "enable a token" for use on the site. Ideally, a person should have a single Principal ID across multiple tokens possibly from different issuing agencies and across card-renewal cycles. For example, an Italian government site may chose to use the national social security ID that is present on all Italian cards. When accepting a foreign card, the site may decide to newly issue an Italian ID for that person or alternatively add some namespace prefix[6] to the foreign ID to guarantee uniqueness in the local domain. In some cases, it may be desirable and possible to verify that two tokens have the same card holder by visually comparing textual and picture data. The module further inserts a subset of personal data in some local user profile repository (implemented as LDAP or DBMS) that is later used for assigning roles and for access control.
- A server-side module that performs the SSL handshake, verifies the CA via IDA's Bridge CA, verifies the certificate, verifies the revocation information (LDAP or OCSP), and returns the Principal ID of the user, either via a lookup of the token ID[7] in the local user profile repository or by a query of some remote service (federated use, Liberty Alliance standard). This isolates web applications from the diversity token IDs by consistently presenting the person's Principal ID.
- A standard interface for a server-side module to look up identity data and roles and access right information from the Principal ID.
- A server-side module that makes access control decisions based on Principal ID and role/access right information in the local user profile. Where this kind of declarative access control is not possible, it interfaces with the application server (for example, J2EE) to support programmatic access control.

Note that different eID initiatives may provide different levels of security. For example, only some registration authorities may require face to face identification of the card holder and only some may use secure messaging. It may therefore be necessary to classify different eID cards according to the security/assurance levels defined in CEN 224 15 in order to provide input to access-control decisions.

5 Families of sites with similar needs can obviously share the same module implementation; national use of a single module is likely for say government services, but Europe-wide use is highly unlikely.

6 An ideal choice for a prefix is the 3-digit international standardized country code (ISO 3166) which is already present on the token as part of the Distinguished Name of the issuing organisation.

7 Usually the CN in the authentication certificate; in some cased part of the CN (e.g., the Italian eID CN also contains a digest)

An impediment to the efficient design of a solution is the poor understanding of the use of identifiers in the eID domain, both for tokens and for persons. Data on which issuers share a common namespace (in which Ids are unique), on the life cycle of the IDs from a given issuer, and from the kind of id (card id vs. person id) used in different certificates would greatly facilitate the design of solutions. If an evolution of eID tokens shall be supported by the software system, a central server that provides this kind of data is desirable.

Proposed Solution

To achieve interoperability in the eID domain, we believe that a tight and orchestrated collaboration between the various national initiatives is necessary. A key deliverable of this collaboration must be the development of middleware that supports all or at least the majority of eID cards.

Benefits of Open Source Approach

From both an organizational and a technical perspective, we believe that an *open source* approach to the development of this software is the ideal vehicle for a rapid development and uptake of a solution to the interoperability problem.

It is important for a successful endeavor that all national eID initiatives autonomously contribute to the development and take full ownership of the resulting common solution. In a collaboration of many governments, it is often difficult to implement a central management of activities or to centrally allot resources for common tasks. This is even more true considering that not all countries will join the effort at the same time. The open source collaboration model is ideally suited to coordinate the efforts of autonomous, self-funded players in absence of a central control. Even more importantly, the resulting product is equally owned by all contributors.

The lack of central control and funding of the organizational approach of open source drastically increases the long term sustainability of the solution. While central funding sources are likely to dry out after some time, a community carried effort is likely to be supported while there is a need for the product. Open source can go hand in hand with a commercial exploitation by SMEs or national technology providers that can add to the economic sustainability. A strategy that activates a large number of private sector players can vastly aid rapid adoption of the technology in various sectors of society.

Confidence in security and quality by all players is a major requirement for the successful use of a common software solution in this domain. Open source is ideally suited in this respect since it permits any player, at any time, to *audit* the security and quality of the code. Even more importantly, national initiatives have the possibility to distribute *certified, national distributions* of the code. Open source thus respects the national autonomy and responsibility of actors while still providing an effective collaboration.

Successful electronic identity management solutions need to universally support all possible client and server platforms. In the modern computing world, the free choice of platforms is increasingly becoming important in order to maximize security and minimize total cost of ownership in various situations. Not only can we observe a significant increase in the importance of alternative operating systems such as Linux and FreeBSD, but these systems also run on an ever increasing number of CPUs and hardware platforms. Then there is a rapid evolution of platforms in the domain of embedded systems, PDAs and smartphones. All of these platforms need to be supported by the common solution. Considering the large number of possible platforms, the possibility of incompatible versions within a platform, and the high number of eID cards that need to be supported, the integration of binary-only modules in support of cards becomes combinatorially impossible. In contrast, the open source approach that allows to compile a single source base for different platforms promises to be highly effective and manageable.

Finally, the open source approach is ideally suited for rapid identification of best practices and encourages rapid adoption of the solution in both the government and private sector. Open source allows to easily integrate the solution with pre-existing and complementary systems and to adapt to local needs where necessary.

Components of the Software Solution

We believe that the proposed interoperability initiative should closely collaborate with the existing open source community. This brings in important resources in the form of expertise and reusable code. The community is also an ideal vehicle for dissemination and uptake.

In contrast to most national governmental efforts, open source projects have naturally taken a perspective of global collaboration and integration of a variety of technologies. While collaboration has been spontaneous and informal, it has been no less effective.

Existing open source projects have already provided both, a good proof of concept for the proposed solution, as well as a large step towards its completion. Most significantly, the ***OpenSC*** project (http://www.opensc.org) whose objective is to interface to smartcards, has already provided an advanced framework for the integration of different tokens and systems:

- it compiles on multiple platforms including Windows, Linux/Unices, MacOS X
- it provides a choice of smartcard reader frameworks: PC/SC[8] or OpenCT, each of which already have drivers for a significant number of readers
- it currently provides support for twelve different smart card operating systems that can easily be extended with the help of expert technical support from the community
- it natively provides access to the objects of self-documenting file system layouts (PKCS#15) and makes it possible to add small modules to access resources on other file systems.

Hiding this wide diversity, it provides a uniform API on top of which smartcard applications can be written. One of the standard libraries above the low-level API that is provided by the project is a PKCS#11 module that enables Mozilla-family Web Browsers to perform SSL-authentication using a smart card. Together with CSP11 (http://labs.libre-entreprise.org/project/showfiles.php?group_id=48) it can also support Internet Explorer.

Ample proof of concept is given by the fact that already, a significant percentage of European eID cards are supported by OpenSC: The official middleware provided by the Belgian and Spanish governments is based on OpenSC and available for download under an open source license. OpenSC further has support for the Finish, and the Estonian eID card, and support for the Italian cards is planned.

OpenSC is the ideal basis for implementing the necessary client-side component for authentication via browsers. What is missing is the addition of support for the remaining eID cards.

Sitting on top of OpenSC, the open source project ***OpenSignature*** (http://opensignature.sourceforge.net) has already prototyped the other two required client-side modules. In particular, it has experimented with a URL Programming Interface (http://prdownloads.sourceforge.net/opensignature/upi-eng.pdf?download) that we believe to be a uniquely suited mechanism to provide access to both identification data and to digital signature services for remote web applications. Among the advantages of the approach are:

- only multi-platform, multi-browser approach we are aware of
- browsers without Java or JavaScript support (e.g., on small devices) are supported; HTTP and HTML forms are the only requirements

8 PC/SC lite is provided by the open source project MUSCLE http://www.linuxnet.com/

- high level of security through a single point of control for access, possibility of security auditing, and guarantees for explicit user consent of certain actions
- consistent user experience of important actions such as digital signing across all remote web applications.

The remaining work consist of the definition and implementation of a standard URL Programming Interface to smartcard services including access to identification data and digital signature.

The ***OpenPortalGuard*** project (http://OpenPortalGuard.sourceforge.net) has been specifically launched to implement the complementary server-side modules of the solution. To achieve this objective, it proposes an innovative architecture for a single-sign-on and access control system optimized for transport level authentication[9] as used with SSL and smartcards. Among the benefits of its design are:

- explicitly designed to support a wide range of eID cards and to map the possibly many issuer-dependent card IDs to a single ID for the person that is invariant over time[10]
- as secure as SSL itself (in contrast to cookie based solutions that break SSL-sessions and rely on cookies as credential)
- less complex than cookie-based systems[11]
- centralized declarative access control that interfaces to multiple application servers of differing technology (J2EE, ASP, PHP, etc.)
- off-loading of CPU-intensive SSL processing from application servers
- highly scalable[12]
- mapping from logical to physical URLs

The project is still in the planning phase, but partial funding has been secured and an initial development/support community is in place.

Summary of Proposed Actions

- Orchestration of a large scale collaboration effort to achieve interoperability
- standardization of the few required interfaces also in relation to work under construction in ISO SC 17 WG 4 TF 9 (ISO/IEC 24727)
- detail design and open source implementation of a single software solution that supports all eID cards
- implementation and operation of possible supportive systems:
    - server to collect and publish the organization of identity information on various cards, the validation mechanisms, and the mapping of the information to the ICAO data model
    - server to collect and publish security levels for different cards (if necessary)
    - server to collect and publish data on ID namespaces and characteristics (if necessary)

9 Traditional single-sign-on solutions are optimized for username/password credentials and implement authentication at application-level that rely on cookies (instead of ssl-sessions) as session concept.

10 At least within the protected site

11 Application servers remain unchanged and need not “collaborate” as in the traditional single-sign-on (sso) architecture, limitation to a single domain as is typical for portals avoids the need for a different cookies from sso server and all application servers, as well as for out-of-band communications between sso server and application servers. Reduced complexity promises higher levels of stability and security.

12 Instead of a single sso server, a parallel array of stateless gatekeeper hosts is used

- supportive studies of selected issues:
    - security audit of various proposed approach
    - study that provides better understanding of the use of IDs

Analysis of Challenges (technical and institutional)

The proposed solution poses various challenges.

Creating the consensus and collaboration among national governments at the scale and completeness required for an interoperable solution is surely not easy. Provided that the need for far-reaching interoperability is recognized, the lack of alternative approaches will be highly convincing. Awareness of the benefits of interoperability, as well as the risks inherent in a lack of interoperability is an important factor for success.

Another factor that can help to overcome the challenge is the informal and gradual character of collaboration typical for open source. Collaboration can start at a minimal level without the need for formal commitments or explicit funds. From there it can gradually be extended to more complete collaboration. Similarly, collaboration can be started by a relatively small number of countries that can gradually grow without rigid requirements on timing. Eventually, peer pressure can help to achieve complete coverage of interoperability.

While collaboration with the community of existing open source projects is crucial to the success of the endeavor, virtual communities usually lack incorporation and thus a clear organizational model with well-defined representatives and decision makers. These projects usually also lack funding and consequently guaranteed delivery times for contributions. In order to incorporate open source projects in a wider collaboration context with well-established organizations, some impedance mismatch has to be overcome. One possible approach is to fund collaboration in the form of contracts with companies that employ key people of the project or individuals directly. The use of open forums[13] (e.g., mailing lists, wikis) in support of collaboration can further help to overcome the impedance mismatch.

On the technical side, we believe to have found good solutions for the key problems. For a wider acceptance and for confirmation of this belief, discussion in a wider circle and peer review would be highly desirable. A thorough security review of the proposed architecture is also mandatory.

While the proposed approach attempts to incorporate all existing eID initiatives without modification, it poses the requirement that certain specification detail of the card must be publicly available. Following the approach of *full disclosure* that is commonly accepted in cryptography and security circles, such publication is common procedure. Not surprisingly, most of the existing eID initiatives have already followed this approach and the key standards for eID cards (CEN CWA 14890, CWA eAuthentication, NIST PIV) require self-documenting cards that follow the PKCS#15 standard. While there seem to be few eID initiatives that keep the card specification secret, we believe that example and peer pressure will eventually convince them to publish the information and join the interoperability initiative.

13 Where possible the ones already used by the projects

Proposed Role of IDABC

We believe that IDABC is well positioned to help make interoperability in the eID become a reality. In particular, we propose that IDABC could consider the following actions:

- create awareness of the benefits of interoperability and the cost of the lack thereof
- in collaboration with other stakeholders such as the Porvoo group and the Global Collaboration forum on eID, help establish and operate the *World eID Steering Committee* [launched December 10 2004 in Prague] that can orchestrate the necessary collaboration, from both a medium and a long term perspective.
- thoroughly review the proposed solution and audit its security
- study the security issues described in the paper

Acknowledgments

Jens Jorgensen, Senior Architect, Tallán Inc, has provided valuable comments and editing that are highly appreciated. Many thanks to the Town of Grosseto and in particular Pier Luigi Bonucci for support of this work.