Achieving Full eID Mobility across Federated Political Domains: a Case for Mobile Identity with Operator and ME/SIM Platform Independence

Chris Porter
CIS Department
University of Malta
chris.porter@um.edu.mt

ABSTRACT
It is the purpose of this paper to introduce the concept of identity mobility within the limited device arena, supported by embedded security, public key cryptography and traditional identity federation mechanisms. This allows citizens (users) to authenticate themselves at a high level of assurance anytime and anywhere using their Mobile Equipment (ME) with *no* operator or device restrictions. A further purpose for this paper is to demonstrate that through an on-going project, SFIMME (Secure Federated Identity Management in Mobile Environments), as a complementary solution to existing and new nationwide eID implementations, cross-border identity mobility may be fully achieved in a democratic federation of peer political blocks.

Keywords
Electronic Identity, Identity Management, Identity Mobility, Federated Communities, Federated Identity, Embedded Identity, SIM Application Toolkit, STK, AVR, Mobile Communities, Identity Centric Mobile Architecture, Security, PKI, Limited Devices, GSM.

1. PROBLEMS IN MOBILITY
Throughout the past few years, a number of initiatives were initiated with the primary aim of achieving identity mobility. In their work, Klein and Hlavacs [1] have identified the important aspect that humans by nature are permanently "*moving between communities*". The authors have suggested a ubiquitous interoperable community infrastructure focusing on the way humans switch between such communities. Klein and Hlavacs have suggested the usage of JXTA for ad-hoc P2P (mobile) computing. Together with the latter, they have also suggested that the telecom operator would be responsible for maintaining user authentication information. These two proposals surely bring forth three main shortcomings:

- *ME platform dependence:* Infrastructure is dependent on the platform used (J2ME) and client tools are to be installed on currently owned device (Mobile Equipment). Binds usage to a particular device.
- *Market Restriction*: Infrastructure is dependent on agreements with a particular telecom operator. This automatically excludes a large number of people/citizens.
- *Authentication Delegation*: User Authentication Information is delegated to third parties (Telecom Operators), which are not within the federation's political sphere.

In a prototype developed at Oslo University College [2], a conglomerate of vendors and other parties have joined forces in order to put forth a proposal for SIM based strong authentication, namely SIM Strong Authentication (StrongSIM). This proposal takes SIM authentication onto internet based transactions, making it an ideal proposition for achieving identity mobility, using the SIM card as a hard-token providing for 2-factor authentication. Founding members, Telenor, Gemalto, Linus and Oslo University College have delivered a prototype based on SS7/IP switching while making use of a telecom operator's HLR (Home Location Register) system for subscriber authentication. This is once again bound to a particular telecom operator, since the HLR is a central operator repository holding subscriber details. This technology is highly coupled with specific operators who agree to participate, and also takes away identity management functionality from the internal community's Identity Providers and delegates it to politically-external operators. This particular scenario can have the following implication: If Federation (F) offers a services (S_1), and operator A (O_A) is an Identity Provider (IdP) within F, a prospective citizen within the community who is a subscriber of another operator O_B , cannot be authenticated in F, unless O_B , joins F. This 'joining' requires O_B and F to carry out a policy mapping exercise, not to mention the technological mapping burdens. Similarly to the work suggested in [1], market restrictions are part-and-parcel of this approach, since only a limited number of operators will join into the Federation, hence leaving out a potentially large portion of the population.
With around 203[1] mobile network operators in the European Region, and an average of 3.9 operators per country, the two proposals discussed above could only be feasible for local and targeted communities, mainly as a VAS (Value Added Service) offered by a particular operator or a small group thereof. Furthermore, this proposal does not make use of the SIM/USIMs cryptographic potentials, since it makes use of basic SIM algorithms (A3, A8 and A5).

Moving on to Finland, it is found that with almost 165, 000 certificates distributed to citizens by the end of 2007 [3], Finland's *FinEID* is now heading towards end-to-end transaction security over WPKI through a SIM-Enabled Open Mobile Payment Platform. This platform builds upon the existing PKI, hence making it easier for the 5 million+ mobile subscribers to utilize. Once again, this proposal makes use of telecom operator-

[1] Including Virtual Operators using other networks – "*List of Mobile Network Operators in Europe*" – Wikipedia 15th February 2008

owned SIM cards for the storage of electronic data and programs. Private Keys are also stored on the SIM card. Once again this approach presents us with a situation wherein users are bound to a specific telecom operator, and automatically excludes any other operators outside the infrastructure. Would this be an ideal scenario for identity mobility, especially across political and geographical borders? The given suggestion of using the mobile phone as a FinEID card terminal, carries with it another drawback:

- JSR177 (SATSA – Security and Trusts Services API), which is used to communicate with security devices (e.g. SIM) as well as to manage digital certificates/signatures while providing crytpo operations, is only partly[2] supported by a minority of ME's in circulation at the time of writing[3].

In his presentation at the ISSE/Secure 2007 conference held in Poland, Marko Hassinen [3] stated that the SIM card belongs to the mobile operator, and out of 4 operators (Sonera, Elisa, DNA Finland and GSM Aland), only 2 have started to distribute SIM cards with the FinEID STK application stored on it. Automatically, this has blocked out subscribers from the other 2 networks to benefit from this proposal. When asked about this, Hassinen agreed on this selectiveness, and argued that hopefully, through an Open Mobile PKI Platform, all operators will start offering such services. Still two problems stand:

- SIM cards have to be re-issued
- Cross-border mobility has not been solved

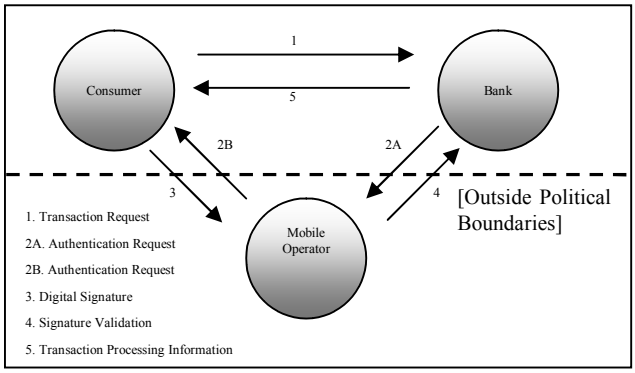

Fig.1 High Level Representation of FinEID

It is important to note that the Authentication Request and Authentication mechanisms are delegated down to the Mobile Operator. Is it politically correct to say that the MO determines who is who? Is it safe to delegate and trust a third party, outside the political sphere? In Finland *TeliaSonera* and *Elisa* are used as the main MSSPs (or Mobile Signature Service Providers), since they are trusted by the parties within the system, including the consumers. Any obvious limitations?

- Only *TeliaSonera* and *Elisa* subscribers can use the services
- System is thus not scalable, unless the MOs acquire other major and global operators
- Mobile Operator acting as the MSSP may not be trusted by all the banks (in this case) or other service providers.
- Banks have to 'leak' information on who is using their sensitive services to Mobile Operators.
    - How secure is sensitive information when stored on MO systems?

Microsoft have recently introduced Windows CardSpace, promising an online counterpart for our physical identity cards as found in a wallet [4]. Based on the .Net Framework, CardSpace allows each card in this virtual wallet to be used in various transactions, at different security levels, depending on the card itself. But how portable is this proposal when compared to the traditional wallet? When asked, Ronny Bjones, Microsoft's Security Strategist, answered that Roaming capabilities will be introduced in the second version of CardSpace in collaboration with Gemalto. In a separate presentation[4], Ksheerabdhi Krishna demonstrated the potential of the Roaming SmartCard Store in CardSpace, wherein it was demonstrated that CardSpace can interact with a smart card reader, getting any identities from a smart card for use within any transaction. When the smart card is removed, any associated identities are also removed from CardSpace. Once again, a smart card reader is required in order to carry out a transaction; to what extent does this solution provide mobility?

Higgins Project, an open source Identity Framework [5] allows for the integration of the various personal identities ('Me') which are required in our day to day lives (e.g. Social, Healthcare, Work and so on). The introduction of I-Cards, which as in CardSpace, could be both personal or managed, allows users to sign-in onto different web-sites without submitting any additional credentials, using a browser based agent. Once again, the question of portability arises. Although based on Java Technology, and thus can be used on various platforms, it still does not secure portability of identity in a transparent and inclusive way.

1.1 ID Mobility and SAML

SAML, especially in its second revision, was a move forward in creating an environment wherein user identity could be federated across political boundaries, and this is shown through the number of initiatives which are currently in development/use: Feide (Federated Identity for Education), Shibboleth Middleware and its applications amongst others.

Morgan et al [8] introduce the concept of cross-institutional Single-Sign-On (SSO) or Federated Credentials on the web, through Shibboleth. This system allows for inter-institutional sharing of restricted resources which are subject to various security access levels. Authorization takes an attribute-based approach, whereby users from a particular institution can access

[2] SATSA API is made up of 4 main areas; APDU Comms. API, JCRMI API, PKI Sig. Services API and the Crypto API. Very few mobile device vendors have actually implemented all of the SATSA stack in their MEs.

[3] January 2007: Nokia marketed the E50 as supporting JSR-177. Only half of the SATSA APIs were actually supported.

[4] "*CardSpace and Smart Cards*" – soap**box** on MSN Video

certain resources hosted at another institution depending on their security clearance which is dependant upon the attribute agreements between the respective institutions. The utilization of Identity Providers and Service Providers allows for the federated security mechanism to be built, allowing users to access restricted resources from other institutions (other than their home institution) using a home PC over an internet connection. This mechanism allows for two or more institutions to share their restricted resources amongst each other's user base, but the more parties are involved, the more complex the configuration becomes.

Mike Donaldson [9] from PingIdentity Corporation explains the concept of Federated Identity as a means for strengthening relationships amongst commercial partners using the same concepts as proposed in Shibboleth for Identity Management.

In June 2006, 16 federal agencies have joined a public-private initiative[5] as part of the US government's strategy to drastically improve the delivery of governmental services to its citizens while reducing costs in the provision of such. The E-Authentication Federation, launched by the E-Authentication Initiative, allows for citizens, business and governmental employees to make use of online services offered by the government's varying agencies. Users make use of e-IDs which are issued by trusted third parties, while a number of Credential Service Providers (CSPs) aid in the management and authentication of the e-IDs through which users may make use of the various E-Authentication enabled online services. To date, 6 CSPs take the responsibility to authenticate the citizens wanting to access the services offered by the different departments, and these include the Department of Agriculture, the Department of Treasury and a number of Designated Financial Agents (DFA's), authorized by the Department of Treasury to offer Credential Services [10].

The term 'Sharing of Identity' theoretically implies user mobility; but to what extent are the current proposals adding mobility to the users and their identities? And to what extent is this promoting secure authentication anywhere?

1.2 ID Mobility: Unanswered Questions

After analyzing all of the above, the following questions still stand:

- How do all of these proposals address identity mobility?
- Do they allow users to actually carry their identity with them, wherever they are, and use it on whichever platform they are operating?
- Can *Identity* be mobile across political, geographical and technological borders without being dependent on any telecom operator, ME, SIM and platform vendor?
- With 27 European countries working on their own eID implementation, how can cross-border mobility be addressed?
- Do we need to delegate Identity Centric and Authentication Processes to Operators or SIM vendors if we need to go mobile?

[5] E-Authentication Initiative launches the E-Authentication Federation (4th August 2006) – Brian A. Doherty

This project demonstrates how Identity Mobility may be achieved in an inclusive manner, through the usage of widely accepted and supported industry standards.

2. INTRODUCTION

During the Ministerial eGovernment Conference in Manchester (2005), the foundations for an EU-wide eID scheme were laid as part of the European eIDM Framework 2010, mainly focusing on eID interoperability and citizen mobility (in service consumption) [18]. Herbert Leitold stated that creating a nation-wide eID implementation for each EU member state was/is the easiest part, but when it comes to making the national "*eID mutually recognized across all other Member States by 2010*", many questions remain unanswered. Interoperability standards and specifications have been agreed, but to what extent cross-border mobility [recognition] has been addressed?

As already stated, a primary objective of this paper is to demonstrate that cross-border eID mobility may be fully achieved in a democratic federation of peer political blocks. SFIMME is intended to operate in conjunction with existing and new national eID implementations, allowing citizens to move across borders together with their fully functional eID as provided by their home political block/node. Interoperability and cross-border eID recognition are two major problems the EU is currently facing when it comes to citizen movement across member states. This work gives a complementary solution to this problem, allowing for free identity movement across political, geographical and technological borders, with Platform and Telecom Operator independence. This work also allows for the separation of the Data Channel from the Service Provision Channel, hence offering additional flexibility and security to implementation strategies
The approach suggested through SFIMME overcomes the current deficiencies in identity mobility, by allowing users to authenticate themselves, in a legally binding way, anywhere.. This authentication mobility is based on traditional cryptographic processes (using Elliptic Curve Cryptography), but introduces the concept of platform and network abstraction. This abstraction allows citizen identities and cryptographic routines to work anywhere the citizen might be at any point in time, while using any ME/SIM combination on any GSM network (with roaming capabilities). Apart from this SFIMME is designed to operate in a multi-channel scenario, thus the citizen is not limited to one particular service provision medium. Data channels could range from a PC with an internet connection to a mobile device with browsing capabilities and also a kiosk with simplistic I/O capabilities. The Security Channel will always be routed through a mobile device (ME) housing an STK enabled 8-bit Microcontroller which is in no way fixed or embedded onto the SIM card or ME. SFIMME allows for the separation of the data channel from the security channel, with the security channel following widely used and accepted standards, including 3GPP TS 11.11, GSM 03.38, 3GPP TS 03.40 and GSM 11.14.

The term 'Identity Mobility' in federated environments is proposed with the integration of four basic concepts into one cohesive system; Embedded Identity, Identity Federation, Distributed and Mobile Communities and Policy. Embedded technologies cater for the citizen's digital identity and identity-centric operations, which incorporate strong authentication mechanisms using public key cryptography. Identity Mobility is

enabled by the abstraction of the user's SIM-card through the utility of an STK-enabled 8-bit microcontroller as mentioned earlier. On the other hand, Distributed Communities are created through the introduction of a Federation Community Process (FCP) in order to create a Democratic environment wherein political blocks (nodes) may;

- Agree on citizen and node certification and rights;
- Submit Trust Revision Requests for both Citizens and Nodes;
- Determine federation-wide attributes and process policies; and
- Manage the community in general through a distributed decision making process.
    - Accept/Reject requests (right of veto)

Mobile Communities are also supported through the utility of embedded identities and SAML assertions. More detail on the above is given later on.

This Identity-Centric Mobile Architecture (ICMA) allows for invisible cross-cultural user movement across varying Political Blocks, Services and Devices in a secure and trustworthy approach. The separation of the Service Provision Channel from the Security Channel allows for a wider range of sensitive services to be provided by nodes within the community. Shifting the Identity Provider authentication processes onto an embedded mobile security device allows for increased digital identity mobility and security with no third party authentication intervention. This potentially also implies a **Transparent SAML Profile**[6] enabling strong authentication with no re-directions as in traditional SAML based applications, and on a separate security channel. This meta-profile can be opposed to all the profiles suggested in the "*Profiles for the OASIS Security Assertion Markup Language (SAML) V 2.0*" [6].

Another primary aim of this work is to take an *inclusive* and *portable* approach; reducing technological and political constraints to a bare minimum, and thus adding operator and device independence to the final solution. This could only be achieved by adhering to widely used and industry accepted standards while abstracting from proprietary infrastructures.

3. OBJECTIVES

The objectives of this work are briefly defined hereunder, in no particular order. Further details are given later on within the *Solution* topics (Refer to Section 4), describing all the elements involved.

- *To Achieve **Full** Identity **Mobility***
- *To **Enable Cross-Border** Transactions*
- *To Engineer an **Inclusive System** with no Discrimination* on:
    - *Mobile Equipment Type and Complexity*: System is to work on all Mobile Devices, from the cheapest to the most expensive.
    - *Mobile Network Selection*: System is to operate irrespective of the GSM network the citizen is currently subscribed to.
    - *Service Delivery Channel*: System shall be capable of handling more than one service delivery (data) channel (e.g. OTC, Kiosk, ME amongst others)
- *To Provide Strong Authentication **Anywhere***
- *To **Eliminate** Delegation of Certificate Management and Authentication Routines to politically-external entities.*

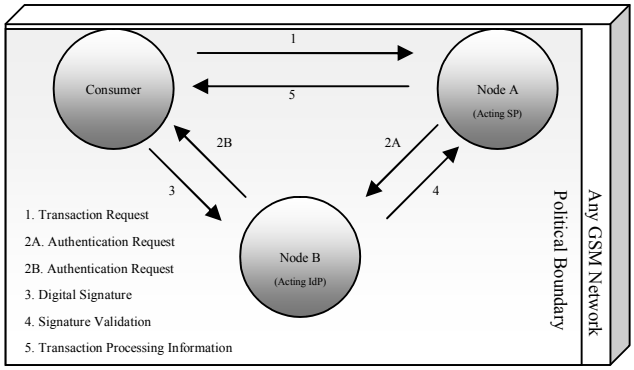

Fig.2 Architectural objective of this project – Everything within political boundaries with no delegation to politically-external entities as shown in Figure 1

In the diagram shown above (Fig.2) Node A is currently an Acting SP while Node B is currently an Acting IdP. Both Nodes have the same roles within the federation (both IdP and SP). It depends on the current transaction to determine which node will act in which role

The above objectives were only achievable through a thorough analysis of the available technological options, and the following are the major areas which were taken into consideration.

3.1 Embedded Identity

Each citizen is a member of a particular node, while also being a member of the wider federation/community. By definition this membership allows him/her to be *'footloose'* in terms of service consumption and also in terms of physical cross-border movement. One way of identifying a legal citizen is by providing each and everyone with a digital certificate, issued and signed by his/her own node within the Federation. Such a certificate is to be presented whenever required during a transaction/authentication process. In the achievement of total mobility, and with current technological implementations, the latter requirement may provide the certificate owner with logistical and security concerns; How can the certificate be presented when not at home/office, and in a public place? Where is it stored? How can it be carried around?

This thesis answers the above question through an *Embedded Identity*, which identity is issued and managed by the Federation's Identity Providers and not by any third party external to the federation's political sphere such as a mobile network operator. Similar proposals have been suggested, but with two major differences;

1) Identities are stored onto a particular network operator's SIM card. This would obviously restrict the number and variety of

[6] A profile where no redirection to the IdP's authentication pages would be required, and where the transport layer would be based on GSM 11.14 and 3GPP 03.40.

users which can be part of the federation, depending on which operators agree to join and act as Identity Providers within the federation. This leads the discussion onto the major second difference.

2) In other proposals, Network Operators act as Identity Providers (handling and/or providing user identities). Why should a network operator act as an Identity Provider in a (e.g.) Banking community? Do all operators have the same level of trust? Shouldn't identity provision and management remain within the community (federation) itself?

For the above reasons, this work introduces the usage of an 8-bit STK-enabled microcontroller which is loaded with the citizen's Identity together with supporting crypto-functionality. This microcontroller is placed on top of the citizen's SIM card, thus abstracting from operator and network dependencies. Current research is also aiming at providing wide compatibility with a larger number of devices, manufactured from 1998 onwards (See 5.2).

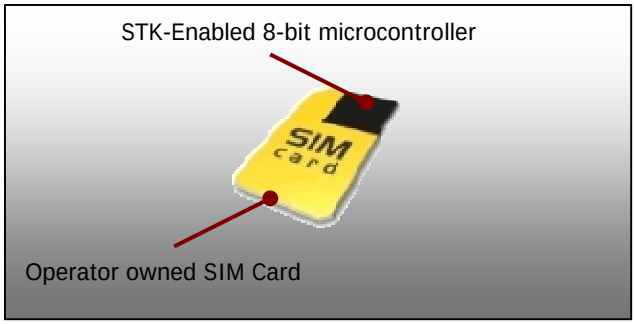

Fig.3 Microcontroller's position on SIM Card

Hence, citizens making use of services within the federation are not restricted by any affiliation to a particular mobile network operator (SIM owner) or network per-se whenever authentication is required. This independence stretches also on the type of device being used. This is due to the use of STK applets, which standard is implemented and *understood* by the majority of MEs, unlike other technologies.

3.1.1 MCU Security

The MC (Atmel's Atmega 128) is protected at two levels, through fuse-bits, controlling what is readable from outside the unit, and also through lock-bits, which through the kernel provided, control which blocks of protected memory each application can read/access, achieving an application-level security mechanism in flash memory. The PROGMEM loader section of the MCU holds what is called the "Protected Memory" (within the Bootloader section), a 256-byte page secured through hardware lock-bits. This portion of memory can only be accessed through the controller's kernel, which checks access rights (ownership) whenever an application tries to access/use a particular block/s (16 bytes each). Symmetric encryption is also possible by storing secret keys in the Protected Memory block using specific encryption permissions. This removes any read-rights, and makes the key (block) usable only for de/encryption purposes only. More data can be written in memory, which is de/encrypted through this protected security-block.

The above security levels allow for the secure storage of the Citizen's Private Keys/PINs into Protected Memory, accessible only through the SFIMME authentication applications only.

3.2 Full Identity Mobility

This work introduces the concept of *'full identity mobility'* in federated environments, by detaching the authentication process onto a separate security channel through the usage and abstraction of existing mobile network infrastructures. This is opposed to the generic approach used in existing Federated Systems, whereby the user is redirected to his/her respective Identity Provider for authentication (using any auth. context) on the same channel (data channel). The latter approach presents technical and security restrictions to the service consumer, for a number of reasons;

- Presentation of security token may be difficult in certain environments
- Security token has to be physically carried at all times to ensure strong authentication alongside with other devices, such as PDA, mobile phone, car keys and so on.
- Service provision may not always be PC based; Kiosk based, WAP based, OTC (Over-The-Counter), Hardware based, amongst others are other potential service provision channels.

As stated in the previous section, this proposal *does not* suggest delegation of identity verification and validation routines onto network operators. A principal assumption is that such parties are external to the political/security domain of a particular community. Thus *network abstraction* is suggested, leaving full authority of identity and its management within the community per-se.

Network abstraction and platform independence is achieved through the introduction of another layer in the Network-ME-SIM communication path. As mentioned in previous topics, the Atmega128 MCU contains the citizen's sensitive information (in protected memory block) as well as the crypto applications, while using the underlying SIM to access any network.

Given that the citizen is a *valid* member of a particular community and that he/she is a subscriber with *any* GSM network operator, this approach allows such citizen to consume services offered within his/her community of federated institutions and/or political blocks using a high level of assurance wherever he/she is and independently on whichever medium the service is provided.

The utility of widely used and accepted standards has led the project to be as inclusive as possible whereby any mobile device manufactured from 1998 onwards is a valid community device. Testing is conducted using a number of devices, with their manufacturing date ranging from 1999 onwards.

3.3 Strong Authentication - Anywhere

This proposal suggests the usage of strong-authentication as follows: Whenever a service consumption request is received at a particular Service Provider's Resource Server, this initiate a Transaction Authentication Requests (TARs) through the respective Identity Provider. This TAR is marshaled to the citizen's ME, whereupon receipt, the citizen is prompted to sign such requests through the automatically triggered STK application

stored on the microcontroller. The signed request is then marshaled back to the IdP for authentication, after which a SAML *Response* is created in response to a previous *AuthnRequest*.

No redirections to the IdP login pages are required, while strong authentication is achieved in a simple two-fold process with no compromise to the citizen identity's security.

The citizen's hard token (8-bit microcontroller) apart from holding the certificate details, will also be responsible for:

- Detecting any incoming authentication requests (TAR) automatically;
- Prompting for user intervention to supply a PIN code
- Confirm transaction;
- Signing requests; and

Sending signed requests back to the Identity Provider.

3.4 Multi-Channel Design

The separation of the Security Channel from the Service Provision Channel leaves no restrictions on the way Services are provided to citizens. Given that the user's ME is the sole authentication agent, it allows for services to be provided on a vast number of channels, ranging from PCs, Public Points, Kiosks, OTC (Over the Counter) and Mobile Devices amongst others.

Consuming a service using a mobile device, the same device with which the user must authenticate, presents no difficulty, since the authentication processes are launched through a different layer from those on which all other ME applications sit (e.g. Browser). STK based Authentication Applications are automatically executed off the microcontroller placed within the device, mimicking the behavior of the citizen's SIM card, while using encrypted information stored in the controller's protected flash memory.

3.5 Trust

This work suggests that *Trust* is built around a communal set of democratic processes, named the FCP (Federation Community Process). Both Service Providers and Identity Providers are to act as peers within this system, allowing for the realization of a distributed environment, at both technological and administrative levels. Trust is achieved when all peers express their confidence and trust levels towards other peers and/or citizens (users) within the federation. A Federation Information System allows peers within any federation to act and interact in a democratic environment, as denoted in the following sub-topic

3.6 Peer Design: Federation Community Processes

Institutions/Political blocks within the federation will have equal weighting and will inter-operate as peers through the introduction of technological processes (FCP or Federation Community Process), enabling a solid political and decision making framework through which a "trust environment" will be built. This trust environment will be backed by a strong community-wide PKI, within which each peer (node) will be issued a digital certificate by the federation CA. Take N_1 as an example, where N_1 is a member and peer within a federation F_1. N_2, N_3 and N_n trust N_1, since N_1's certificate is not in the Distributed CRL. In this scenario, N_2, N_3, and N_n will also trust N_1's citizens, since such citizens will be issued a certificate using N_1's root certificate. If N_2 decides that N_1 has breached some clause, or for any other reason decides that it won't trust it (and its users) anymore, N_2 may initiate a Trust Revision Process against N_1 through the Federation Information System. If all peers agree, through a forum-like interface, and accept N_2's decision, then N_1's root certificate is placed within N_2's CRL[7] and is no longer trusted by the other members. Consequently, N_1's citizens will not be able to consume services offered by the other federation members.

The usage of JXTA is proposed for the FCP[8], although it is still pending implementation. Peer services offered through the Federation Information System or FCP are as follows

- *Node monitoring*: Determine status of other nodes, including Activity and Trust Levels. Generic Node Information is also provided, such as addresses, contact information and so on.
- *Add Node Request*: This allows all the existing nodes to accept a new node within the community. All nodes or a percentage thereof (depending on the policy adopted) have to accept this request, which request is initiated by any existing node representative.
- *Trust Revision Requests*: Any node can initiate a Trust Revision Request against any other node. This request is electronically distributed amongst all the nodes present in the federation for them to consider and act upon. If all nodes agree on such revision, then the certificate of the node in breach will not be trusted anymore (revoked). This denotes the need for managing a distributed Certificate Revocation List integrated by a global OCSP, wherein each node within the community publishes its own CRL, with a list of non-trusted nodes (certificates, if any). Such distrust is automatically propagated down to any certificates issued by such Node (Citizens/Devices). This revision by consent allows all the nodes to have an equal say in the federation. Feedback and discussion on such revisions may take place in a forum-like space.
- *Attribute Addition/Revision System*: This sub-system allows nodes to decide on citizen attributes in SAML transactions. Such attributes carry with them a specific Security Level while each citizen will have one or more attributes associated with him/her. At each transaction, the attribute with the highest security level will be taken into consideration in determining whether such citizen has enough rights to consume the requested resource (See 3.8). This is an important aspect, which can make or break the validity of cross-border eID movements.
- *Grapevine*: At 3 main levels; Political Level (Node Management/Leadership), Administrative Level (Node Technical Staff) and Citizen Level. At each level, different

[7] Which makes part of a distributed CRL (OCSP)

[8] JXTA-Overlay [19] denotes a clear example of JXTA's capabilities in meeting SFIMME's requirements for a Federation Information System or FCP, which includes Peer Monitoring, Peer/Resource Discovery/Allocation, File/Data Sharing, P2P Communication (e.g. Rooms) amongst other capabilities.

but relevant discussions may be going on, with access dependent only to the specific security clearance of the citizen in question. Such forum will allow for a discussion space at both the node level and also at the community level. The grapevine is to provide Shared Repositories for documents and other resources.

The Federation Community Process creates a democratic environment wherein all nodes act and interact in one level of authority, sharing information and decision making processes, creating a transparent environment for mobile citizens to freely move across nodes (borders).

3.7 Policy

In this proposal, *Policy* is translated into the agreement and mapping of process policies, authentication policies and security assertions between segments. This also encompasses the mapping of the various security policies as required by any PKI, including the Certificate Policy (CP), Certification Practices Statement (CPS), and the setting up of a governing Policy Approval Authority (PAA). Moreover, in this case the development of a policy concerning the processes involved in embedding identities and the respective crypto-functionality on hard-tokens is also important.

The latter involves the utility of specific hardware which will enable the citizen's private key to be loaded on his/her hard-token for later use, together with the required STK authentication/signing applications.

3.8 Transaction Based Security Level

Each Service Provider is responsible to determine the security level required for the consumption of a particular resource. Each citizen has associated with his/her home account a number of attributes (e.g. Student, Academic, Administrator), with each attribute carrying a particular security level, as in the following example:

Table.1 Community-wide attributes and Security Levels

Attribute	Level
Student	1
Academic	2
Administrator	3

When the citizen requests a resource, the authentication process will primarily determine whether an attribute with a security level greater or equal to the level required by the resource is associated with his/her home account. If the citizen has an attribute carrying the requested security level, then the TAR (Transaction Authentication Request) will resume with strong authentication over the citizen's ME (Mobile Equipment). As an example, if a Student wants to consume a resource aimed at Academics, he/she will be prompted about the transaction's invalidity.

4. SOLUTION

This section describes the solution proposed, starting off with a textual scenario, describing the system's flow, and important alternatives. Following is a breakdown of the infrastructure's elements, together with technical descriptions and results obtained.

4.1 Elementary Textual Scenario

This section will describe a real-life application scenario for this proposal: A *Bank Service Authentication scenario within Federation F_A, with the Government (GOV_1) acting as an Identity Provider and the Bank (B_A) as a Service Provider.*

- **Version**: 1.0
- **Actor**: Citizen C_1 in FA

4.1.1 Normal Flow

1. Citizen C_1 requests a service from Bank B_A. Both know that they are within F_A.
2. B_A requires the highest level of Authentication for Service S_1 and asks C_1 for his Node ID (Where are you from?) and his personal Home ID (in this case, his ID Card Number).
3. C_1 returns these details to B_A.
4. B_A checks C_1's Security Level against the required security level for this particular service (using the published web-services found at the citizen's IdP's EPR). If citizen does not have enough privileges, the process stops here.
5. B_A determines whether C_1's issuing certificate is trusted within the community. If yes, proceed to step 6, else process stops.
6. B_A asks GOV_1's Identity Provider (IdP) to authenticate C_1 at Level 3 (Strong Authentication) through a SAML Authentication Request.
7. GOV_1's IdP initiates the authentication process by invoking an STK application on C_1's mobile device with the transaction details.
8. C_1's STK application is invoked with transaction details, and allows C_1 to examine the details. He/she then signs details by clicking on OK after entering a PIN code. This will invoke a signing algorithm which makes use of an embedded Private Key. If C_1 decides not to sign, the process stops here, and a time-out is recorded.
9. The signature is sent back to GOV_1's IdP which is in turn validated through normal signature validation routines.
10. If Valid, GOV_1's IdP will send back a simplified Authentication SAML Response to inform B_A that C_1 is whoever he/she claims to be together with multiple SAML assertions defining C_1s role/s in the community. Full SAML Response is stored at the IdP's tables for reference.
11. An acknowledgment is sent back to C_1.
12. Given GOV_1 trusts C_1, and B_A and GOV_1 are in F_A, then mutual trust exists, and the transaction is authorized.
13. C_1 consumes S_1 to an extent as allowed by C_1's attributes.
14. C_1 could also be provided with a session on B_A's services pages with respective restrictions, once again as allowed by C_1's federation attributes.

4.1.2 Alternative Flow

1 to 7. As above

8. C_1 rejects authentication request by any of the following:
    A. Clicks on Cancel
    B. Ignores Message
    C. SIM Abstraction Layer (Security Module) is not present in the ME

9. If A or B occurred, STK application registers C_1's actions (GSM 11.14 – Transaction ended by user or transaction timed out) and sends back a rejection notice to GOV_1's IdP. If Security Device is not present skip to 11B.
10. GOV_1's IdP informs B_A that C_1 has not accepted the request.
11. Depending on the above:
    A. BA denies access to S_1.
    B. GOV1's IdP times out transaction and B_A denies access to S_1

4.2 SFIMME Prototype Building Blocks

The following are some details on a number of research areas within this project.

4.2.1 Citizen eID Token

An 8-bit Microcontroller with STK capabilities was chosen to house the electronic identity together with authentication applications (ECC signing algorithms). The selection was based upon a number of alternatives, each of which was tested against a number of factors:

a) Availability of development tools (AV)

b) Range of client devices which support technology (MES)

c) Extent to which standards are followed (ST)

d) Acceptability of standards used (AST)

e) Cost of development tools (CDV)

f) Development Accessibility (DA)

g) Technology learning curve required (LC)

The following were some of the options considered:

Table 2. Comparison of major GSM 11.14/3GPP TS 03.40 compliant hard token technologies

Manufacturer	AV	MES	ST	AST	CDV	DA	LC
G&D (StarSIM Platform)	Med	Med	High	High	High	Low	Low
G&D (UniverSIM JavaCard)	High	Med	High	High	High	Low	Med
Gemalto USIM cards	Med	Med	High	High	High	Low	Med
Bladox TSIM	High	High	High	High	Low	High	High

The above table denotes a summarized comparison of a number of major SIM/UMTS technologies which could be used as hard tokens in SFIMME MEs. The MES column denotes the number or range of devices which are capable of '*understanding*' crypto functionality written in Java, C or any other platform dependent language.

As one can seem TSIM from Blaodx offered the highest MES. This is due to the fact that applications for such token are written in an STK API written in C, thus making them available for the majority of devices supporting STK (1998 onwards). The Development Accessibility (DA) column denotes the development ease and real network testing capabilities, whereby applications development can be carried out without the need to rely on any particular mobile network operator. Given that this technology abstracts the SIM-ME interface, all it needs is any valid SIM card from any subscriber. Also, the DA and CDV for TSIM are based on the fact that all development APIs and documentation are freely available as part of an open source effort. Hardware required for development is comparatively offered at a low price.

The LC is quite high, since there is a very small development community using it, and the APIs are not widely used for PKI implementations.

On the whole, the 8-bit MCU offered by Atmel and enhanced through Bladox's APIs, showed to be the most promising option for this project. The following are some further details with this regard.

4.2.1.1 8-Bit STK SIM Extension vs. JavaCard SIM

6th of April 2007 - WPKI.net announced that the WPKI specification based on WIM technology was 'abandoned'[9] and is now favoring the SAT (SIM Application Toolkit) based solution. This decision may have been defined as drastic by mobile manufacturers, but will surely benefit the end-user and consumer in general.

To date only a few hand-picked devices support WIM based solutions, and supporting technologies such as JSR-177 (SATSA)

At the time of writing, no mid-range mobile device (excluding emulators), supported all the APIs defined in JSR-177 or SATSA (Security and Trust Services API). Nokia, a world leader device manufacturer presents[10] API support information for their device platforms, and the following tables are extracts from such, showing the area of interest, that is, the support Nokia devices provide to SATSA APIs.

Table 3. Nokia Series 40 JSR-177 Support

	2nd Edition	3rd Edition	3rd Edition FP1	3rd Edition FP2	5th Edition
SATSA (JSR-177)				**APDU only**	**APDU and CRYPTO**

Table 4. Nokia Series 60 JSR-177 Support

	1st Ed	2nd Ed	2nd Ed	2nd Ed FP2	2nd Ed FP3	3rd Ed	3rd Ed FP1
SATSA (JSR-177)						**CRYPTO and PKI**	**CRYPTO and PKI**

On the other hand, STK or SIM Application Toolkit is a GSM standard (GSM 11.14), which is supported by the majority of devices and is also in use by most of the GSM network operators for Value Added Services (VAS). (U)SAT (3GPP 31.111) is STK's 3G counterpart, and both are supported by the majority of devices, allowing for services to be un/loaded securely onto the SIM by the operators. This is all done independently of the handset. STK Event triggers allow for SIM application activation, including calls (both incoming/outgoing), messages, call timers and mobile location. In this case, all applications will be triggered from the MCU, rather than from the SIM card itself, although the same concept is used.

[9] http://www.wpki.net/ - 6th April 2007

[10] As at 25th May 2007

Allowing for low level development with simplistic UI, STK and (U)SAT can also be used in fairly complex menu-based systems.

Thus the latter approach was chosen, in compliance with WPKI's decisions, whereby STK would be the main driver for WPKI operations and application development in SFIMME. This also provides:

- Manufacturer independence
- Cheaper solution making use of existent technologies.
- Inclusive technology rather than an exclusive higher-end market technology (business phones/PDAs).

STK alone does not ensure network independence, but combined with the STK-enabled 8-bit microcontroller 'abstraction' layer within the Network—ME—SIM stack, this independence is achieved.

Continuous research is currently being made on STK's adoption in modern devices and smart cards. Vendors such as Gemalto and G&D are developing new smart cards which will facilitate the development and management of applications upon such, using widely known development platforms, such as .Net and Java, with better security, enhanced storage and presentation capabilities. In all cases, STK stays present at the lower levels of the development platform, be it .Net based and/or Java cards. This was confirmed by Gemalto after the .Net Gemalto Card was exposed during their presentation [7] at the 2007 ISSE/Secure Conference hosted in Warsaw.

4.2.1.2 GNU AVR-GCC

In this work, the development of crypto-functionality and request handling facilities for the 8-bit microcontroller (Atmel ATmega128) is carried out using the AVR-GCC C compiler and assembler licensed under the GNU Project. This, together with STK APIs for C provided by Bladox, a research entity based in the Czech Republic, allowed for the development of all the STK applications required to abstract the required functionality from the operator owned SIM card.

This area of research is crucial in achieving full identity mobility, since it is the only enabler for movement across ME platforms, Networks and SIM card platforms. Adherence to industry accepted standards including 3GPP TS 11.11, GSM 03.38, 3GPP TS 03.40 and GSM 11.14, is considered as a very important factor in this work.

4.2.2 Nodes – IdP and SP Stacks

The second important factor in this work is the concept of Nodes, and not distinct Identity Providers and Service Providers. In this work it is suggested that all Nodes act as both *IdP*s and *SP*s, in a peer environment, whereby each node is responsible for its own *citizens*. This means that when citizens from Node *A* are consuming services from Node *B*, *B* will ask *A* to authenticate its own citizens, while at the same time *A* may also offer services to its own citizens and any other citizen within the community of peer nodes. The concept of peers denotes that all nodes have an equal say in the community through the various Federation Community Processes (Refer to 3.6). This allows for better community growth and easier policy mapping, reducing as much as possible any hints of political power struggle.

As explained above, the federation, or community of nodes, will be made up of equally significant nodes, all acting as both *IdP* and *SP* at the same time. This reflects the real scenario, wherein all political blocks in a federation might be responsible of a number of citizens (*IdP*), while providing services to such, and potentially to other citizens from within the community (*SP*).

Although the design requires an *IdP* and *SP* stack at each node, it is not required that such functions are operative in all of the nodes. A node might provide Identity information without offering any services itself and/or vice versa. If a particular node decides that it needs to activate any of the two stacks (*IdP* or *SP*), this would entail no additional configuration, since each node would have the two stacks present and readily active. In the case of activating the SP Stack, the node technical team would be required to develop the respective SP services and simply integrate the SP Agent (refer to 4.2.2.2) for authentication mechanisms. In the case of the IdP stack, citizen eID tokens have to be issued using the provided hardware based issuer, together with certificates issued from the local CA.

4.2.2.1 Node IdP Stack

The *IdP* stack is made up of the following elements:

- **GSM Gateway**: Acts as a gateway between the *IdP* server and the citizen eID token housed in the *ME* (Mobile Equipment).
- **Certificate Authority:** Issues citizen keys and certificates. Private keys will be stored on the citizen eID token, while certificates will be managed through a LDAP service.
- **Citizen eID Token Loader:** Hardware[11] and software which enable the initialization of citizen eID tokens with private keys and supporting authentication software.
- **Authentication Web Service**: All nodes are able to carry out citizen authentication through an authentication web-service mechanism. If citizen from node *A* wants to consume a service from node B, and node B requires strong authentication, then node B will ask node *A* to authenticate the citizen. This authentication will be carried out through authentication web services exposed by the IdP stack at the respective node (*A*). Once authentication is completed (successful or not) a serialized simplified Authentication Response for the original Authentication Request is sent to the relying Service Provider. This SAML Response is furthermore modified into a simpler markup (SSPML) for use by the SP Agent (Refer to 4.2.2.2), providing authentication status, basic citizen information and basic IdP contact details. The full SAML Response object does not cross the network due to its size, and is stored locally on the respective IdP's DB. This design consideration was taken in order to provide a lightweight approach to traditional SAML assertions, and in order to enable mobility.
- **SSPML:** A simplified SAML Response or Simplified Service Provider Markup (SSPML) syntax is introduced

[11] Bladox BXTOP45P (USB/SIM/MMC card dev. kit.), based on ATMEL ATMega128L MC and FTDI FT8U245BM for USB connectivity.

for this purpose. The reduction of network traffic allows for this system to be used while traveling using a mobile device (roaming).

```
<AuthenticationResult>
     <Subject>
         <Name>Chris</Name>
         <Surname>Porter</Surname>
     </Subject>
     <AuthnStatus>100</AuthnStatus>
     <Attributes>
         <AttributeID>1</AttributeID>
         <AttributeID>3</AttributeID>
     </Attributes>
     <Issued>2008-01-02T17:34:21.893Z</Issued>
     <IdentityProvider>
         <Name>Node One</Name>
         <SupportEmail>support@node1.com</SupportEmail>
         <SupportAddress>NodeOne NDO1</SupportAddress>
         <HelpDeskNo>+356 2345 3321</HelpDeskNo>
    </IdentityProvider>
</AuthenticationResult>
```

SSPML Response as received by the SP Agent from the Identity Provider. Attribute IDs are resolved through the usage of local SP services[12]

- **SFIMME Database:** A local partition of the overall distributed database. This holds details of the following entities
  - *Citizen***:** Local citizen information. Can also be constrained to existing institutional tables.
  - *Attribute***:** A list of attributes as agreed by the whole community. These are automatically kept in synch throughout the community. Each attribute holds a security level (e.g. Student at Level 1). Such level is then used for authentication purposes.
  - *CitizenAttribute***:** A many-many relationship between attributes and citizens, defining what Attribute/s each Citizen has.
  - *Node***:** Community-wide Node information. This information is kept in synch throughout the community.
  - *SAMLTransaction***:** Holds all SAML objects (Requests/Response) pertaining to all transactions passing through the current Node.
  - *Transaction***:** Transaction logging.
- PostgreSQL (v. 8.2) was used in order to construct the data layer.
- **LDAP Server:** Based on OpenLDAP, provides LDAP services for local node citizen certificates. These are used before and during signature verification processes in valid authentication transactions (Not yet implemented).

4.2.2.2 Node SP Stack

The SP stack is made up of the following Elements:

- **SP Services:** A set of services are offered through servlets at the SP Stack. These servlets offer facilities such as:
  - *Retrieve Community Nodes*: Retrieves a list of active Nodes within the community, together with their respective EPR (Endpoint Reference). This list is then offered to citizens during the authentication process, allowing them to select their Home Node (Identity Provider) before initializing the authentication process.
  - *Retrieve local Node-ID*
  - *Retrieve Node's community code*
  - *Request User Authentication*: This service receives authentication requests from the SP Agent, which in turn creates a SAML Authentication Request Object. This is then serialized and sent as a parameter to the published Authentication Web Service (Refer to 4.2.2.1) of the respective IdP.
  - *Check Node's Trust Status:* Checks whether a particular node is trusted by the community. This is carried out through an OCSP check against the distributed CRL.
- **SP Agent**: An SP Agent acts as an interface between multiple SP applications and the Service Provider servlets provided within this stack. This allows for multiple and different applications to be offered at one SP, which applications are not bound to implement authentication routines. All that is required is a call to an agent with a number of parameters, including:
  - *Home Node:* Selected by the citizen
  - *Citizen Home ID:* Submitted by the citizen
  - *Security Level Required:* Dependent on current authentication scope. If resource being requested requires that the citizen satisfies a minimum security level, then this level is passed to the Agent. The agent, before initiating the authentication process, will check with the IdP (citizen's home node) whether the current citizen satisfies the minimum security level required by the resource. If the citizen has an attribute with a security level which is equal or greater than that required, then the process continues, otherwise the Agent notifies the SP application accordingly and aborts authentication.
- Multiple agent types are provided for each Node, allowing Service Providers to build applications for diverse platforms. SP Agents are to be provided in:
  - **ASP.Net 1.x and 2**
  - **JSP/Applet**
  - **Lightweight Agents for Mobile Devices**
- If citizen satisfies the required minimum security level, then the authentication process continues. If this is

[12] Attributes are synchronized across all nodes, including the respective Security Levels

successful, a temporary cookie is created, which cookie is then used by the base service application to create a session with any data as required (e.g. User Details and Time of Authentication). This cookie is automatically deleted immediately afterwards the session is created.

- Alternative approaches are also being analyzed, since through the above approach, not all browsers behaved uniformly.

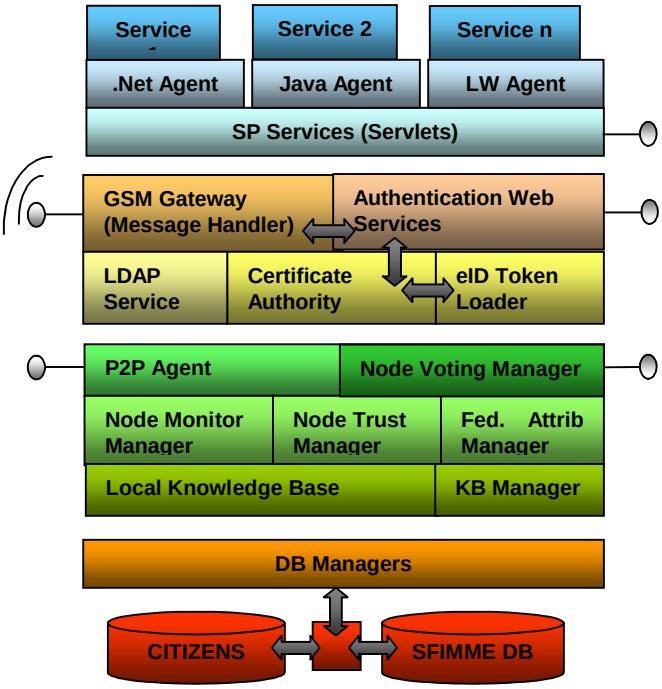

Fig.4 Anatomy of a SFIMME Node (Top: 1. SP Stack 2. IdP Stack 3. P2P Stack 4. DB Stack)

4.2.3 P2P Stack (Not Implemented)

The Point to Point Node Stack represents the technology responsible for linking all the Nodes together, while keeping the distributed data in synch across the community. As seen in figure 2, the P2P Stack is composed of the following elements:

- **P2P Agent**: Responsible for sending/receiving data and requests from/to other nodes within the community.
- **Node Monitor Manager**: Responsible for detecting active nodes while mapping them for a graphical overview of the community. Basic information will be made available next to each node, including:
  - Node ID
  - Node Status
  - Certificate Status
  - Number of Citizens
  - Number of Services Offered
  - Contact details
- This data is updated in real-time through the P2P Agent
- **Node Trust Manager**: This manager is responsible for the handling of trust revocation requests and response messages (Refer to 3.6).
- **Federation Attribute Manager**: This manager is responsible for mapping and keeping community attributes in synch, together with their respective security Levels. This would ensure that a particular node won't need to assess what each and every attribute means, but will base its authentication decisions on the respective security level required, which is agreed upon before the attribute is accepted within the community framework. Note that each transaction is based on a particular Security Level.
- **Node Voting Manager**: If during a voting phase (e.g. Node Trust Revocation Request or the introduction of a new Attribute), one particular node votes against or does not accept any revisions, then the Node Voting Manager will be responsible for informing all the other P2P agents of the node's decision. Unless all Node Voting Managers (or a % depending on the policy) in a community do not publish a YES vote for a particular motion, then the process will not be executed (e.g. New Attribute will not be included within the distributed SFIMME DB).
- **Local Knowledge Base (Forum)**: This forum holds all the discussions pertinent to the local Node, at 3 distinct levels: Political Level (Node Management/Leadership), Administrative Level (Node Technical Staff) and Citizen Level.
- **Knowledge Base (KB) Manager**: Responsible for making local knowledge available across the community. If someone at Node A looks up for information at a community level (not just locally), then the KB Manager at each node will be responsible for returning any relevant and meaningful information from their respective local KBs.

Why do we need to distribute? Couldn't the KB be global, immediately? It is important to keep in mind that distributing technology also means distributing power, in both political and technological terms. Who will take responsibility to host anything? Why would Node A host and manage data for Node B? This approach ensures extensibility of the system, with little room for power friction amongst separate nodes or political blocks.

4.3 Current Implementation Status

Partial implementation of the system was carried out at the University of Malta.

The following diagram depicts the current status; areas shaded in gray are still pending implementation. All other areas, including the SP (Blues), IdP (Browns) and DB Layer (Reds) have been implemented in order to proof their feasibility.

To date, it was concluded that the overall proposal is achievable with the technology used.

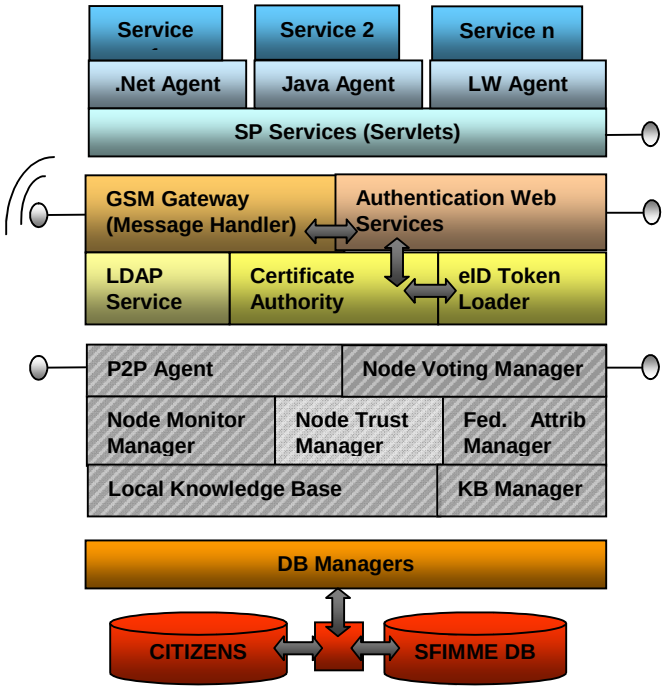

Fig. 5 70% of prototype is implemented as at January 2008

With the current status, mobility could be proven, and the following diagram depicts the steps the system takes in order to verify and authenticate a mobile citizen when trying to consume a service offered by a node other than his home node.

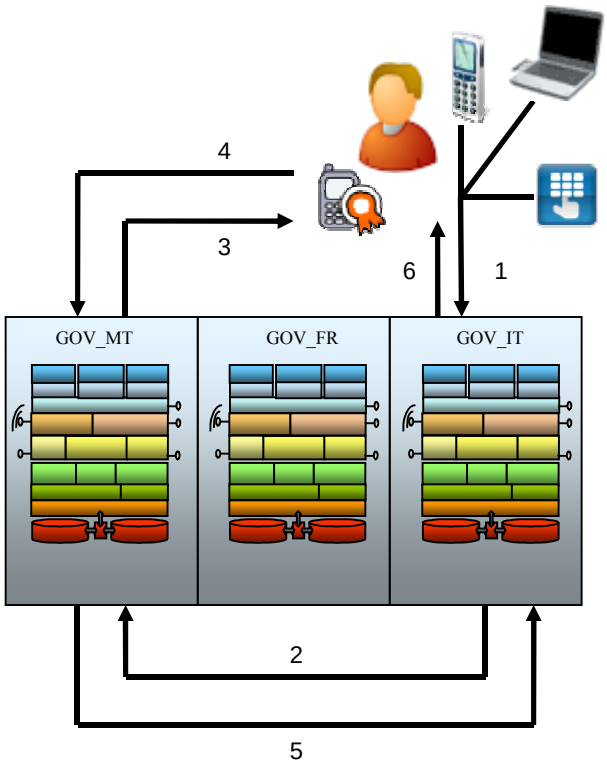

Fig. 6 Roundtrip achieved by prototype (as at Jan 2008)

4.3.1 Citizen Requests Resource/Service

At this stage, a federation citizen requests a particular service or resource from a SP within the community. He/she is not challenged with any username/password authentication, but is asked to select his/her home node from a given list, together with his/her home identity (e.g. ID Number/eID number/Telephone Number/Student Code etcetera). After doing so, such data, together with the required security level for the current resource/service) is then passed to the SP Agent which is now responsible to initiate the authentication procedure.

This step could be carried out through any service provision channel, either over a PC, over a Mobile Device, Kiosks, OTC (Over the Counter) and so on.

4.3.2 SP Agent asks questions

Before proceeding, the SP Agent will check whether the chosen IdP is trusted by the community, through the distributed CRL (Refer to 4.2.2.2). If not, the process will terminate here, as no citizens from that particular node are allowed to consume any resources/services from that or any other node across the federation.

On the other hand, if the chosen node is trusted, the Service Provider Agent (any platform), will ask the chosen Identity Provider (e.g. Government of Malta eID) whether this citizen has enough privileges (security level) to consume such service (through his/her attributes).

If the citizen has no attributes with a security level equal to or greater than that required by the Service Provider for the current

service/resource, the citizen's home node will return a simple response indicating this fact (Refer to 4.3.5).

On the other hand, if the required security level is satisfied, then the Identity Provider will initiate the authentication process, by sending a SAML Authentication Request.

4.3.3 IdP – Citizen Verification

At this stage, the Identity Provider will initially check whether the citizen has a valid certificate (using local CA routines). If, not, this fact is returned to the relying node (Refer to 4.3.5).

On the other hand, if the citizen holds a valid certificate then the process resumes as follows:

1) The Identity Provider creates a transaction ID
2) Using this ID together with citizen data, it formulates a simplified BER-TLV[13] array, as shown below:

```
[OMMITED SMS HEADER]
//6//NODE_ID
//4//"GOVMT"
//TRANSACTION_ID
//2//5
```

3) This message is then sent to the citizen's ME for verification and authentication (Refer to 4.3.4).
4) IdP waits for citizen's response. A time-out occurs if no reply is received from citizen after x seconds (specified from the Node's configuration).
    a. If a time-out occurs, this is logged into the system and reported back to the relying node (Refer to 4.3.5).
    b. Otherwise the IdP carries out the process as specified in section 4.3.5.

4.3.4 Citizen Verifies

An STK application on the citizen's ME will pop up in the foreground (irrespective of the current activity on the ME), asking the user to verify the given transaction (Transaction ID). If the citizen is the owner of the transaction, then he/she will click on verify to complete the authentication process, after submitting a PIN code.

This step will digitally sign the Transaction ID, which signature is then sent back to the Identity Provider (still waiting for a reply unless no time-out has occurred).

If the citizens' ME does not launch the STK application for any of the reasons listed below:

- eID Token not in place,
- SIM card not in place,
- ME is switched off,
- No Network Signal,

… the transaction will cause a time-out, and the process terminates.

[13] Basic Encoding Rules – Type Length Value

The signing algorithm used on the token is based on Elliptic Curve Cryptography (EC-DSA) and was based on LibTom's LibTomCrypt [14] cryptographic toolkit.

4.3.4.1 Citizen eID Token: Why ECC?

The limited device arena poses a greater challenge when it comes to identity management and crypto functionality. Since this proposal promotes the embedding of identity and crypto-functionality onto an 8-bit microcontroller as part of a wider PKI, it was important to define resource parameters for the hardware being used. This is an essential exercise where limited resources are available, making an addition of 1Kb to the software footprint an expensive proposition.

4.3.4.2 Computational Efficiency

In cryptographic terms, although ECC arithmetic is more complex it still offers the highest strength-per-bit [15] with the smallest key size when compared to any non/commercially used public-key scheme. This is an important factor when resource availability and processing power is limited.

Although ECDSA is based on DSA, Johnson and Menezes [16] have shown that the former has various advantages over DSA, such as feasibility in "*restricted computing environments*".

4.3.4.3 Key Size

It is generally understood that a longer key size makes a cryptosystem more secure. On the other hand, the longer the key is, the more resources are required in order to:

- Generate keys (if required)
- Store the key
- Process signatures
- Communication overhead

Elliptic Curve Cryptography carries a high level of security at a smaller key length. A detailed discussion on this area can be found in the complete text [21].

4.3.5 IdP Verifies and Reports Back

If the process has reached 4.3.4, then the IdP would still be waiting for a reply from the citizen. If no reply is received after a pre-specified period, a time-out occurs. If this happens, the IdP will report this back to the relying node, and the current transaction is logged appropriately.

If a reply is received from the citizen, the following will take place:

1) IdP will verify signature using the citizen's public key obtained through the local LDAP service.
2) A SAML Response is generated according to the results achieved above (Non/Authenticated) and stored in the SFIMME DB in conjunction with the SAML Request.
3) A Simplified Service Provider Markup (SSPML) Response is generated, based on the response generated above, and marshaled back to the relying SP.

In any case, the following is the list of all the possible SSPML response statuses which the acting IdP Node may return back to the relying Node.

- Citizen Authn: *Authenticated* (100)
- Citizen Authn: *Pending* (50)

- Citizen Authn: *Not Authenticated* (-100)
- Citizen Authn: *Timed Out* (0)
- Citizen Authn: *User Does Not Exist* (-110)
- Citizen Authn: *Not Enough Privileges* (-120)
- Citizen Authn: *Citizen Certificate is Invalid* (-130)
- Citizen Authn: *Node Certificate is Invalid* (-140)

A SSPML response is sent back with any of the above codes. Basic citizen information is only passed when status is 100.

4.3.6 Relying Node – Session Management

Once the SSPML reply is successfully received from the acting IdP Node, the acting SP node will now possess a simple XML document with all the details required in order to manage the Citizen's requests. The following questions may be answered through the SSPML response:

- What is the transaction status? (Refer to 4.3.5)
- Is the citizen trusted?
- Does he/she possess enough privileges to consume this resource?
- What is the name/surname of citizen?
- What are his/her attributes?
- When did the citizen authenticate (timestamp)?
- Who issued the response?
- What are the basic contact details of the issuer?

Using the above information, the acting SP Node may create and manage a session (if required) for the current citizen. IdP information may be required in order to direct the citizen to appropriate contact details if help would be required, or if any problems with his/her eID token occurs.

The SP Agent (.Net based) creates a temporary cookie on the current machine, so that the base application could make use of the given information. Once the session is created, this cookie will be automatically deleted for security purposes.

It might be argued that this is not the preferred approach, but session management is not central to this work and it is left up to the SP Application developer/s to manage user sessions (e.g. In Process, on DBMS, using cookies, etcetera), if required. This system may also be used for a simple Yes/No answer, with no particular need for session management, allowing instant access to a particular resource only if the citizen is who he/she claims to be and with specific privileges (e.g. Physical Access Control).

5. CONCLUSION

Through SFIMME, total identity mobility has been achieved using the mobile device as a host for a fully portable eID token, backed up with a solid network of peer nodes acting as both SPs and IdPs as required, per transaction. This has been achieved through the selection and adoption of widely accepted industry standards which have been in use, and will be supported in years to come. STK is a case in point, whereby it opened up the potential user base for this system to a much wider audience, irrespective of the mobile device used and also irrespective to the mobile network the citizen is currently using. The use of a microcontroller *piggy-backing* the SIM card has also allowed for operator independence, which increases the potential user base. This is obviously a critical success factor for a nation-wide and cross-border eID implementation.

The eID token used is compatible with the majority of SIM/UICC (3G) cards. This approach ensures that the operator's SIMs are not modified in any way (no applets installed).

This system (SFIMME) is not exclusive to existing eID solutions, but is complementary to such. It adds strong authentication capabilities whenever and wherever 'traditional' eID cards/tokens have little or no use (e.g. unavailable card readers, in public points, while on the move). This means that apart from their national eID cards, citizens might opt to carry their eID with them even while roaming across borders, making the ME and 8-bit MCU the primary security channel for cross-border transactions.

Peer node design has allowed for a democratic environment, with all nodes having the same weight in terms of political and technological importance. A modular design approach has helped in achieving this democratic community, while enabling organic growth, whereby the number of nodes is **not** restricted, and nodes can be easily added through a democratic process: FCP – *Add Node Request* (Refer to 3.6).

PKIs at both community (Global) and node levels (Local) have allowed for better trust mechanisms, whereby nodes may determine whether to trust other nodes and their respective citizens, in a transparent way. This was achieved through local CRLs and a published global OCSP.

A live test was conducted; the following is a full description of the test conducted, followed by actual results.

5.1 Results

A roundtrip test for a web-based SP application was carried out. This included all the necessary steps to carry out a full authentication procedure, from SP site loading to the receipt of the transaction confirmation message on the ME, as follows:

5.1.1 SP Site loading

A dummy SP was created (Dummy Bank SP), within which a login module is provided for a particular service.

Fig. 7 SP (Dummy Bank SP) login page

Within the login module, the following is the data required:

- **Where Are You From (WAYF)***:* Select the IdP from a list provided (populated through the SP services). The selection (e.g. *Government of Malta e-ID*) is transparently translated into the respective EPR or End Point Reference indicating the location where the selected IdP has its web-services published.
- **Source ID***:* The citizen's home identity number/code (e.g. eID number).

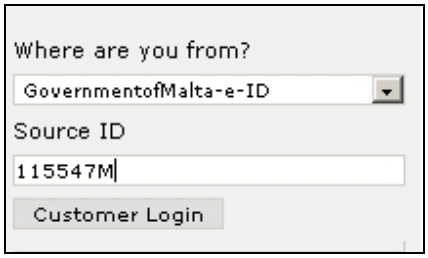

Fig. 8 Home ID basic ID details submitted

The above details, together with the the Security Level required for the current resource/service are passed to the SP Agent as described in the following sub-section.

5.1.2 SP Agent Invoked

The details submitted in 5.1.1 are passed onto the SP Agent, together with the Security Level required for the current resource/service. The SP Agent is in turn responsible to carry out the authentication process with the chosen IdP.

Fig. 9 Agent initiates with pre-set citizen's home IdP and ID

As soon as the citizen is ready, he/she hits on the **'Start Authentication'** button. This invokes the authentication web-services on the chosen identity provider (IdP) for the current citizen. The following checks are carried out before authentication on the ME (Mobile Equipment) starts (refer to 4.3.2):

- Is the chosen IdP a trusted community node?
- Has the citizen got enough privileges to consume the current resource/service?

If the above are answered positively, then the SP generates a SAML Authentication Request and the IdP proceeds by initiating the ME authentication, as follows.

5.1.3 ME Authentication initiates

At this stage, an STK application is invoked on the citizen's ME. A tone is also played to draw the citizen's attention towards the mobile device, while an "Authenticate Transaction" message is shown. After 2 seconds, the transaction ID is displayed on the ME's display.

Fig. 10 Transaction ID is displayed for informational purposes

Hitting on OK, the user will be prompted to submit his/her PIN number. This number is determined by the citizen at the time of registration. Potentially, this could also be combined with the SIM's PIN number, depending on the policy established within the community. A number of drawbacks may exist if the PIN code is combined with the SIM's PIN:

- Erroneous PIN entries may lock SIM card
- Not all mobile subscribers choose to lock their SIM with a PIN, thus this may be easily forgotten.

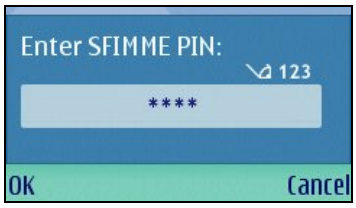

Fig. 11 Submission of PIN

If the correct PIN is submitted, then the citizen is asked to confirm the transaction.

Fig. 12 Transaction confirmation

If *Yes* is selected, the transaction is signed using the citizen's Private Key (which was stored on the Protected Memory block within the MCU at time of registration (refer to 3.1)). This signed transaction is then sent back to the Identity Provider.

Fig. 13 User asked to allow SIM to use network

The last step sends the signed transaction back to the Identity Provider which in turn verifies its validity as described in the following step.

5.1.4 IdP Authenticates signature

As soon as the IdP receives the signature, it is verified using the citizen's public key. If this results as a valid signature, that is, the transaction has been signed correctly using the citizen's private key, then a SAML Response is created. This response is stored within the IdP's transaction tables, upon which a simplified XML (SSPML) response is created (Refer to 4.2.2.1), and is marshaled back to the SP Agent.

5.1.5 SP Agent Receives Response

The Agent will parse this response and display the transaction's success as shown in the following diagram.

Fig. 14 Authentication Successful

After clicking on the OK button (in the case of the .Net based Agent), a session is created for the current citizen using the SSPML (Service Provider Markup Language) response from the IdP.

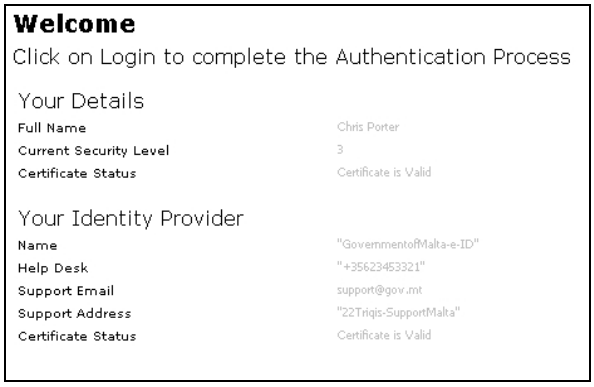

Fig. 15 SSPML data used in newly created session

The SSPML response contains the following details, upon which a session *may*[14] be created:

- Transaction Status (Refer to 4.3.5)
- Citizen Full Name
- Current Transaction's Security Level
- Citizen's Community Certificate Status
- IdP Name
- IdP Help Desk Telephone Number
- IdP Support Email
- IdP Support Address
- IdP Community Certificate Status

IdP related information is used for referential purposes only, and could be used by both SP and Citizen in case any difficulty (at any stage) arises within a transaction (e.g. Error message containing contact details).

In this case, an *InProc* session is created basing on the above response.

Fig. 16 Logged in at Security Level 3

If the Citizen tries to access a resource requiring a higher security level than the one currently authenticated with, another authentication process would be essential, this time with the new Level of Assurance (LOA or Security Level).

5.1.6 Transaction Completed

This concludes the test roundtrip. A receipt is sent back to the citizen's ME using a Flash (or Visor) message type, as shown in the following screenshot.

Fig. 17 Transaction Successful receipt on Citizen ME

[14] Session may not be required in one-off transactions (e.g. Downloading of a specific document or in Physical Access Control)

5.2 5 platforms under test

A test has been conducted using 6 different platforms (i.e. combinations of ME and Networks/SIMs). During these tests, measurements have been taken to identify any discrepancies in authentication timings and success across heterogeneous ME/SIM platform variations. The following are the results achieved, with each figure based on an average over 3 transactions:

Table 5. Timing Results Achieved

ME	Software Revision	IMEI	Network	Seconds*	Success
Nokia 3330	V 04.50 12/10/01 NHM-6	350693801612514	Vodafone	27	√
Siemens A65	V 15 23/03/2005 Variant: A135	35-4494-00-631209-1	Go	22	√
Nokia E50	V 06.41.3.0 24/10/2006 RM-170	351892010286099	T-Mobile	26	√
Sagem myX-1 Trio	NA	NA	Go	40	√
LG KP202	02/2008	354912012109821 00	Go	22	√
Samsung SGH-C100	01.65.AS C10XEWI3 2003	352362004180160 00	Go	27	√
Sony CMD-Z5	6.4.7 SAT* BR:R48ue+w16	350094/40/088925/8	Vodafone	25	√
HTC TYTNII	Windows Mobile 6.0				

* Average test results are based on 3 test-roundtrips per platform

5.3 Errata

- STK Application has a waiting tone with a 3 second duration value [17]
- Human-ME Interaction varies per-transaction. To minimize this discrepancy, a simplistic UI has been provided with a single click at each prompt.

6. BENEFITS OF APPROACH

The following benefits are derived from this work:

A) eID Mobility in cross-border movement

B) Platform (SIM/ME Independence)

C) Strong Authentication Anywhere

D) Mapping of democratic processes into simplistic P2P technological processes

E) Separation of security channel from data channel

7. POTENTIAL IMPLEMENTATIONS

Usage of this system could span to the following user groups:

- Citizen Mobility
  - In conjunction with national eIDs
- Mobility for Specialist User Groups
  - Legal
  - Health
  - Political
- Education
  - Research
  - Resource Sharing
  - Student Mobility (e.g. Erasmus)

8. DRAWBACKS

The following are some drawbacks pertinent to the suggested system:

- Network Roaming Costs (per transaction)
- Due to its experimental nature, the hard-token may denote a higher initial investment, unless economies of scale are achieved.

9. FUTURE WORK

Future work may encompass NFC (Near Field Communication) and the introduction of Sub-Nodes within the same architecture.

9.1 NFC – Near Field Communication

This may enable a better user experience in cases where transaction speed is required. Obviously, the incorporation of NFC would not exclude the usage of STK type messages for transaction processing on the ME. This would provide the user 2 methods of authentication, depending on the situation at hand:

- **Over The Counter/Kiosk transactions**: In this case NFC would be a quicker alternative
- **Internet Transactions**: STK Application invocation through the usage of SIM Toolkit SMS messages.

NFC might introduce the need for token readers at specific points, and for this specific reason it does not contribute to this thesis, where Citizen Mobility is a central philosophy.

9.2 Sub-Nodes

The concept of sub-nodes would be required in larger communities (e.g. EU), whereby nodes may be structured in a hierarchical way, with sub-nodes (Regions) reporting to parent nodes (Country), and in turn parent nodes would report to their own peers.

10. REFERENCES

[1] Bernhard Klein and Helmut Hlavacs, A SEAMLESS MOBILE COMMUNITY SUPPORT SYSTEM, Pervasive 2005 Doctoral Colloquium, 2005

[2] StrongSIM, Offering SIM Strong Authentication to Internet Services, 3GSM WORLD CONGRESS, FEBRUARY 2006

[3] Norbert Pohlmann, Helmut Reimer and Wolfgang Schneider, SIM-Enabled Open Mobile Payment Platform Based on Nation-Wide PKI FinEID, Vieweg, 2007

[4] Ronny Bjones, BelgiumUser-centric ID management & the business impact of 'Cardspace @ work', Microsoft EMEA, 2007

[5] Anthony Nadalin, Eclipse Project Higgins and Identity 2.0, IBM, 2007

[6] OASIS, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005

[7] Gemalto, Strong Authentication as Business Enabler, ISSE/Secure 2007

[8] Morgan, Cantory, Carmody, Hoehn, Klingenstein, Federated Security: The Shibboleth Approach, EDUCASE Quarterly, November 2004

[9] Mike Donaldson, How to Strengthen Your Partner Relationships with Federated Identity, Ping Identity Corporation, March 2006

[10] Brian A. Doherty, E-Authentication Intiative launches the E-Authentication Federation, August 2006

[11] Offering SIM Strong Authentication to Internet Services, October 2006, http://www.strongsim.com

[12] M-Banxafe; secure payment and banking on GSM, https://www.m-banxafe.be

[13] Hans Eberle, Nils Gura, Sheueling Chang Shantz and Vipul Gupta, Cryptographic A Processor for Arbitrary Elliptic Curves over GF(2^m). Technical Report. Sun Microsystems, 2003

National Security Agency, The Case for Elliptic Curve Cryptography, Central Security Service, http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm

[14] LibTom Crypt Developer Manual http://libtom.org/?page=features&newsitems=5&whatfile=crypt

[15] Hans Eberle, Nils Gura, Sheueling Chang Shantz and Vipul Gupta, Cryptographic A Processor for Arbitrary Elliptic Curves over GF(2^m). Technical Report. Sun Microsystems, 2003

[16] Don B. Johnson, Alfred J. Menezes, Elliptic Curve DSA (ECDSA): An Enhanced DSA, Proceedings of the 7th conference on USENIX Security Symposium, 1998 - Volume 7

[17] Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface – GSM 11.11

[18] ISSE/SECURE 2007 Conference Report, September 24–27 2007

[19] Fatos Xhafa, Raul Fernandez, Thanasis Daradoumis, Leonard Barolli, Santi Caballé, Improvement of JXTA Protocols for Supporting Reliable Distributed Applications in P2P Systems, Lecture Notes in Computer Science, Springer Berlin / Heidelberg

[20] Chris Porter, “An Identification and Technical Investigation of a Ubiquitous System for the Provision of Secure Services on Limited Devices in a Federated Environment”, Thesis (To be published in July 2008)