Towards a Pan European e-ID Interoperability Infrastructure

Arnold van Overeem  
Capgemini  
arnold.van.overeem@capgemini.com

Jos van Oosten  
Q-tips  
jos@qtips.nl

Abstract

The proliferation of e-Services in most European Countries has been favorable to the emergence of common identity providers and national identity management infrastructures in these countries. The STORK project aims to interconnect all of these identity management infra-structures to form a Pan-European federated e-Identity space. In this paper we show that due to two different identity concepts in use by the European countries, this objective is a far from trivial challenge.

Based on our analysis we present two scenarios: homogeneous interoperability for countries with alike identity concepts and heterogeneous interoperability for countries with different identity concepts. For the latter case we present three solution directions to overcome technical limitations and challenges.

The STORK project is co-funded by the European Union and will deliver real solutions by implementing five demo projects.

1. Introduction

In recent years significant progress has been made with the introduction of e-Services by public administrations. Although the ambition set by many governments in Europe [1] has not yet been achieved, many countries now have e-strategies [2] that aim to enable secure access to their e-Services for businesses and citizens. 7 countries are deploying eID cards and 14 more are currently designing eID cards for future roll-out. 14 countries have public sector controlled PKI schemes in place. 15 countries use multilevel authentication schemes for public services [3].

Many e-Services store data about persons and require identification of the person who wants to use the service. This identification is needed to select the correct data that apply to the person requesting the service, but also to protect his privacy. Some services require a payment for the delivery of the service, and some services are related to long term base registrations that may affect the future relation between a citizen or business and public administrations. Many e-Services only provide access to registered users. Examples of e-Services that require identification and are candidates for cross-border access are: building permit request handling; subscription to university education; application for a driving license. A prioritized list of relevant e-Services has been developed by the European Commission [4].

Depending on the nature of the service, some degree of certainty must exist that a person who wants to access a service is appropriately identified and authenticated. For identification and authentication of users identity systems have been developed and alongside with these, identity management schemas. In many public e-Services persons could have several roles, e.g. be citizens, or business representatives or public servants. Access rights to services depend on the role of the person, and are generally managed by the providers of the services.

Traditionally each service provider or even each service had, in order to implement proper access restrictions for its services a proprietary identity management function, resulting for the users in an ever growing number of access codes to remember. With more and more services becoming e-Services the need for a common identity management infrastructure has become apparent [5], and this is the subject of the present paper. Identity providers as trusted 3rd parties that assure service users’ identity to multiple service providers have emerged as a solution. The STORK project aims to setup a Pan-European identity management infrastructure, that will enable citizens to have a single registration of their identity at a recognized identity provider and use the services of this identity provider to access all e-Services in all EU-Member States and associated countries.

This ambition either makes the assumption that it will be possible to establish a Pan-European identity service, or to define a Pan-European standard for identity providers. In both cases the resulting identity management infrastructure must be capable to provide authentication with an adequate assurance level to any public e-Service across Europe.

The underlying assumption is that there is a priori agreement about the nature of identity itself; this however is being challenged [6]. This paper reviews the fundamental differences in identity concepts, and in the way identities can be managed, and explores what
requirements an identity provider must fulfill to be compatible with an e-Service.

Based on our analysis we describe the generic relation between an identity provider and an e-Service provider [7]. As described by Birch, Elliott and McEvoy [8] two fundamentally different relationships exist, which have implications for the way e-Services can be supported by an external identity provider. In line with Martens we have dubbed these the “blue model” and the “green model” 2.

In this paper we propose a procedural gateway as an enabler for cross-model interworking between e-Services and identity service providers, as well as three different interim approaches that do not depend on a procedural gateway. We assume that interoperability concepts are relatively independent from identification procedural gateway. We assume that interoperability different interim approaches that do not depend on a procedural gateway. We also assume that the interoperability concepts for e-Identity are independent of the nature of the e-Services that require some form of identification.

2. The nature of e-Identity

Identity is a subject of intense debate and research in the European Union for a number of years now [9]. In this paper we will restrict the discussion about identity to people in any role. Some of the concepts and solutions also apply to legal entities and/or to animals and goods (e.g. ship-containers), the main differences relating to identification / authentication methods.

Identity in the e-Services world usually is defined as a unique set of facts about a person that make him distinguishable from all other persons [10,11]. This definition has two flaws, which limit its usability in practice:

1) Until all other persons have been identified, it is not certain that any given set of facts is really uniquely applicable to the single person of reference. In some cases however, the degree of uncertainty can be significantly reduced by the availability of certain metadata about the facts.

2) Data that represent facts about people may have different and unknown degrees of veracity, both because some described facts may change over time, or because the quality of the information itself is imperfect. This imperfectness can be due to inaccuracy, misinterpretation, misunderstanding and/or deliberate falsification, and further be complicated by the notion that a person may not want to reveal some facts in order to protect his privacy.

For practical purposes “standard” sets of facts about a person have come into use as source of identification. Name (Family Name, Given Name), place and date of birth, is a commonly used set of identifying facts that turns out to be sufficiently unique in most cases and is generally believed to be invariant over time and legislatively neutral.

To address the veracity issues of identifying facts about a person, a plethora of other facts than the commonly used ones have been proposed and practiced, generally classified in knowledge related facts, possession related facts and biometric facts. An identification verification scheme based on a combination of facts out of all three classes, or at least two classes is usually called “strong authentication” and is currently believed to guarantee a higher degree of veracity then a simple validation scheme based on a single class of facts.

In traditional daily life identifying facts support the person of reference, but do not replace him. In e-Services however, the person himself is not involved, and an identity record, containing or referring a set of facts about him acts as a substitute for the person in his relation to e-Services. This different role of the identity record, makes the veracity of the data much more important, and the vulnerability to identity related fraud much higher. The government, as a large provider of e-Services therefore is a stakeholder for quality assurance of identity records2.

This raises the question who owns identity records. In most countries legislation has been passed [12] that sets restrictions and requirements to organizations holding collections of personal records, but in most cases the ownership of the identity records is not clearly or not uniformly defined [13]. In subsequent years the evolution of identity management has come to two different and contradictory views on the nature of identities in a (government owned) data store:

1) The identity record describes an identity which is an attribute assigned to a person in order to function as the digital representation of that person in one or more contexts

2) The identity record describes a person directly and may contain artificial attributes assigned to him by an identity service provider in order to represent him.

The latter approach places the identity provider as the master source of control, and rather would make the person an incarnation of the identity record. The

1] The terms blue and green do not have any other meaning then to reference the two fundamentally different concepts of identity that are discussed throughout this paper. This paper does not intend to express any preference for either concept, nor tries to present a comparative overview of the two.

2] In this paper we mean with identity records any data recorded about a person in order to enable his authentication; this is a subset of personal records in general; we use the term credentials to denote another subset of personal records: the data required to grant or deny authorization to an e-Service.
identity provider defines and controls identity records, even when the service user “pushes the buttons”. His role often is limited to the selection of services and to validate his identity record. Typically each person is attached to one identity record, that may contain a wealth of privacy sensitive information, depending on what is required by various services. We call this the “blue” paradigm or “blue” model.

The former approach typically places the person himself as the master source of truth for the use of identity records. The person self is in control of identity records, and the identity provider is used to validate its content. A person typically can have multiple identity records, which may or may not share identifying facts, and that can be used in different contexts or for different roles that person may have. We call this the “green” paradigm or “green” model.

In the “green” paradigm it is feasible that a single person “owns” multiple identities, typically related to different roles of that person, and it might be difficult or deliberately impossible to relate the provision of different services to that person by different service providers, when these services where obtained using different roles. In the “blue” paradigm the sharing of the same identity record by multiple service providers would make a composite profile of the person much easier, and thus it would be much more difficult to maintain the privacy of the person. In the blue model a person’s privacy is totally dependent on legislation and its flawless implementation.

In both models a priori trust relations are supposed to exist between the user and the identity provider, as well as between the identity provider and the service provider.

2.1 Identity Management according to the blue model

In Figure 1 a simplified schematic overview is given of a service delivery implemented according to the blue model. The model is simplified as much as possible. Essence of this model is that the identity provider represents the service user. The identity provider does not have to be a system, but can be any type of digital asset, the operational characteristics of which, are controlled by the identity provider. The service user can have any form, including internet access, mobile access, access by means of a call center, etc. The service user must be authenticated prior to the service request handling. The service user is not involved in the exchange-of-credentials dialog, and therefore cannot immediately control what facts about himself are revealed to the service provider. Often a policy can be established at the identity provider. Based on this policy the service provider will either get all requested facts about the service user registered at the identity provider, or the service request will be canceled.

It is to be noted that the identity provider has access to information about the service request that the service user issued, also when the service is denied, and therefore has the possibility to collect facts about the user that can be used in future service requests. Because a trust relation is assumed between the service user and the identity provider this does not have to be a problem. However, this fact makes identity providers a prime target for identity related criminal engineering. The user therefore is for the protection of his identity and credentials totally dependent on legislation and the proper implementation of it both at the identity provider and the service provider.

![Figure 1 - Identity provision in the blue model](image)

Each identity provider will usually support only one single instance of the service user, and the service user often is limited in his choice of identity provider by the identification methods that the service provider supports.

2.2 Identity Management according to the green model

In Figure 2 a simplified schematic overview is given of a service delivery implemented according to the green model. Again the model is simplified as much as possible. Essence of this model is that the user is in control each time a service provider asks for proper identification. The identity provider is not involved in the service request and delivery and the service user can decide when credentials are asked whether to authorize the provision or potentially select an alternative identity provider or cancel the service request.

It is to be noted that the service provider is not aware, which identity provider will be selected by the service user until the identity provider fulfills the credentials request on behalf of the service user. The
authentication of the service user takes place after the inquiry for credentials by the service provider. Because a trust relation is assumed between the identity provider and the service provider, the service provider can rely on the veracity of the credentials. Because this model implies a competitive position for identity providers, it is likely that identity providers in this model will support highly customizable and granularly configurable services. By allowing and enabling to expose different credentials to different service providers, the privacy of the service users can have a high degree of assurance. Identity related crime in this scheme is much more difficult, as is the identification of criminals on the basis of profiles.

Figure 2 - Identity provision in the green model

3. Scope of research and approach

In this paper we analyze the interoperability of identity providers in a cross-border situation where service user and service provider operate under different legislative contexts and each have a different trusted identity provider.

For focusing our analysis, we used the layered interoperability model proposed by van Overeem, Peristeras and Witters [14], which is consistent with the European Interoperability Framework (EIF) [15,16] and resembles the layer cake proposed by Berners Lee [17,18]. In this model four layers of interoperability are defined, named from top to bottom: procedural, semantic, technical and trivial (see Figure 3).

The bottom layer defines network infrastructure and connectivity functions. We also assume a fully developed technical layer that handles any syntax, formatting, language substitution, currency and measures conversion, and similar requirements. Any interoperability issues of the service provision context that causes or triggers the identity provision has been considered outside the scope of our research.

We assume that the minimum assurance level of an identity doesn’t depend on the service provider or the Member State for the same class of services. If for example for the service “selling wine” the only identification requirement is to prove that the service user is at least 18 years of age, this is assumed to be applicable for all wine selling services in all Member States, and by implication that the name and place of birth will never be required by the service provider for this type of service.

In this paper we concentrate on the semantic layer and the procedural layer only. The semantic layer describes the exchange of meaningful information by transposing messages with retention of meaning across different semantic contexts using a common or compatible business process. The procedural layer describes the interaction patterns required to enable dissimilar or incompatible business processes to collaborate for a common goal, in this case identity provision in order to support e-Service authorization. This restricts our research topic to the exchange of identity related information in the context of a well defined service request, for which a well defined form of authorization, based on a well defined degree of identification is required.

Figure 3 - Layered Interoperability Model

In section 4 we discuss the application of semantic solutions between identity providers using the same business process model. In section 5 we describe the application of procedural solutions to handle the interoperation of identity providers using different (incompatible) business processes. Whereas section 4 and 5 describe generic solutions, section 6 describes a specific solution for providing identity in the absence of an appropriate implementation of a procedural layer, by using the semantic solutions from section 4 in combination with supplementary implementations specific to identity provision.

Once a service user has been identified (and possibly strongly authenticated), the service provider obtains some facts about the service user, sometimes beyond what is required for identification or minimum verification of credentials.
This paper does not make assumptions about the veracity of any facts about persons that may appear in personal records, nor about its usability to support service delivery to that service user. This paper also doesn’t discuss what legal requirements would apply to the service provider or the identity provider with regard to the handling of these personal data.

In the rest of this paper we will purely focus on the interaction patterns between different identity providers, where one of them is trusted by the service user, the other by the service provider, and the identity providers are subject to legislation in different Member States. We will also not consider the degenerate case when the service user and the service provider use a common identity provider, as this case is assumed to be solved within the national context of the identity provider.

4. Homogeneous Interoperability

We will now explore the complications that must be overcome in order enable cross-border service access. In our simplified model it is assumed that in each Member State a trust relation exists between the service user and an identity provider in that Member State, as well as another trust relation between the service provider and an identity provider in the other Member State. Each trust relation represents a business contract based on the applicable local legislation. As a consequence, cross-border service delivery requires the collaboration (interworking) of two different identity providers.

In this section we will discuss the situation when both identity providers operate under the same model (either blue or green). We have called this homogeneous interoperability. In the next section we will then discuss interoperability between identity providers operating under different models, which we called heterogeneous interoperability.

4.1 Homogeneous interoperability between identity providers in the blue model

In this section we will first discuss interoperability between identity providers both operating under the blue model. A simplified interoperability scheme for the blue model is shown in Figure 4.

In essence the interaction between the service user and the identity provider in the source country is unchanged; authentication of the service provider takes place before the service request is forwarded; also the interaction between the identity provider in the target country and the service provider is unchanged. Added is an interaction pattern between the identity providers in both Member States.

As both identity providers assume the same semantics about the identity concept the exchange of credential updates (step 7 and 8) may not necessarily require semantic conversion. Alternatively interaction (7 and 8) may need to be routed via the semantic gateway. By having the service request (step 3) be semantically converted into a service claim (step 4) the behavior and business rules to be applied by the identity providers in both Member States are unaffected. A so-called semantic gateway [19] is capable to do that job. This semantic gateway mimics a generic service provider to the identity provider that is trusted by the service user, and mimics a generic service user to the identity provider that is trusted by the service provider. In addition it maps the requested service to the corresponding service at the service provider. As both identity providers use the same identity concept and implement compatible or even identical business processes to support service provision, the semantic transformations can be on a message basis and only depend on generic metadata of the service users and the service providers.

4.2 Homogeneous interoperability according to the green paradigm

We now consider the case of interoperability between identity providers when both operate according to the green model. In Figure 5 a similarly simplified interoperability scheme for the green model
is shown. Again the interaction between the service user and the identity provider in the source country is unchanged; authentication takes place after the identity provider has been requested to endorse the claimed credentials; also the interaction between the identity provider in the target country and the service provider as well as the interaction between the service uses and the service provider is unchanged. Added is an interaction pattern between the identity providers in both Member States.

The semantic gateway must be involved in the original service request (step 1,2) in order to create a context for credential mapping. Step 3, 7 and 9 also may have to be routed through the semantic gateway, in order to map between different service contexts in both Member States. As in the blue scenario a semantic gateway may do the translation job, but this would be a totally differently configured semantic gateway as in the blue case.

Like in the blue model both identity providers use the same identity concept and implement compatible or even identical business processes to support service provision, the semantic transformations can be on a message basis and only depend on generic metadata of the service users and the service providers.

5. Heterogeneous Interoperability

In this section we will explore the situation of interoperability between identity providers operating under different paradigms, i.e., one operating under the green model, and the other operating under the blue model.

5.1 Interaction cases

From the description of the homogeneous interoperability cases it is clear that interoperability between a green and a blue environment is significantly more complex. On the service user side the interaction pattern and the role of the identity provider must be maintained in accordance with either the blue or the green model, whereas on the service provider side the interaction and role of identity provider according to the other model must be mimicked. In particular the moment that authentication is required becomes more complex. This situation of dissimilar business processes has been described before [20] and requires the intermediacy of a so-called procedural gateway.

We have two cases: a blue service user accessing a service from a green service provider, or a green service user accessing a service from a blue service provider. In both cases a conversion of business process (as apparent from the interaction pattern) in combination with semantic matching of data from the identity record is required. A semantic gateway cannot interfere with the business process, by definition, therefore a procedural gateway is required.

In the case of a blue user accessing a green service provider the procedural gateway must emulate a green user mapped to a blue identity provider to the green world and a blue service provider mapped to a green service provider to the blue world. The blue user is requested to authenticate prior to forwarding of a service request, and the procedural gateway must store the service user's credentials until in a later process stage the green service provider needs it.

In the case of a green user accessing a blue service provider, the procedural gateway must simulate a blue user to the blue identity provider and a green service provider to the green world. In this case the procedural gateway must store the (potentially mapped) service claim until authentication has taken place by the identity provider in the blue service domain.
5.2 Discussion

The STORK project aims to be a generic solution for all cross-border e-Identity requirements. As shown in this paper four different cases exist, two of which are dependent on the implementation of a semantic gateway and two others on a procedural gateway as well as a semantic gateway. As the procedural gateway is a technical novelty, it is not proven that it can be built, and more precisely that it can be built within the allotted budget and timeframe of the STORK project.

Further complications arise when stepping back and considering the real environment. In reality individual service users access many different service providers in multiple Member States to obtain a variety of services. In our models we have disregarded the possibility of (back-office) interaction among service providers, in particular when this interaction involves personal records of the service user. An example of this would be the registration of a marriage between citizens of a blue and a green Member State in either a green or blue country. In a homogeneous blue or green environment this situation does not require any special consideration beyond what would be applicable within a single country operating that model, but in a mixed blue and green environment it does.

When collaboration between a blue and a green service provider happens, green service providers can be fed with “blue” identity records of green service users. This results in facts being exposed to the green service provider that would not have been exposed in a homogeneous green environment, and thus compromises the privacy of the green service user, and since green service providers are not generally used to protect user data they generally don’t get, green identity providers become a more likely target of identity related crime, making the green service user more vulnerable to identity fraud.

Conversely, blue service providers can be fed with green identity records about blue service users. Generally blue service providers cannot recognize these records as belonging to the same blue service user and therefore must assume it to be a different service user, or take the risk to merge service data from different users. In both cases this may result in inconsistent, duplicated or even erroneous service delivery, and in both cases legislation may be violated if single delivery of the service is mandatory. An example of this is the delivery of digital tachograph card to a truck driver.

6. Directions to solve semantic identity mismatches

From our discussion about interaction patterns between service providers operating across blue and green models, it follows that the political requirement to achieve Pan-European e-Identity interoperability goes beyond what can be done with just ICT solutions. An obvious political way out of the conflicting requirements of the blue and the green model is that all stakeholders agree to adopt either the green or the blue model as the national standard model. We believe that this is not going to happen. Both “green” and “blue” Member States already have too deeply invested in legislation and technology [3] to accept conversion either from green to blue or from blue to green. In many cases citizens already possess digital assets, either in conformance with the green or the blue paradigm, and many third parties already hold digital records with personal data implemented in conformance with either blue or green legislation. Our conclusion is that we either find a technical solution between green and blue identity models, or we embark on a degraded alternative.

A generic and broadly acceptable, technically feasible interoperability solution between green and blue environments requires the development and deployment of a procedural gateway as well as further elaboration. As, in view of the before mentioned complications, this can be impeded by legislative barriers, some degraded solutions can be implemented that avoid the complexities of the cross-environment solutions described in section 5, at least for an interim period.

These interim solutions suppose the parallel development and deployment of two Pan-European e-Identity spaces that cover the blue and green Member States, respectively, but put the burden of the incompatibilities between the green and the blue environments outside the domain of ICT interoperability solutions, into the domain of the stakeholders. So far we have identified three different types of stakeholder who can be burdened with the interoperability conflicts between green and blue environments.

1. The service user can be targeted as a potential contributor to an interim solution.
2. The service provider can be targeted as a potential contributor to an interim solution.
3. The government in its role as legislator can be burdened with the interoperability problems.
This approach transforms the cross-border interoperability case into two parallel homogeneous interoperability cases as described in section 4 (both blue and green).

6.1. Dual identity provision for service users

The basic idea of the first solution is that a blue and a green interoperability world do coexist. Several Member States already are committed to either the blue or the green model. Ultimately, each Member State either implements the blue or the green model and the associated homogeneous interoperability solution as described in Figure 4 or Figure 5, respectively. In addition, service users, that require the use of services from the other domain will be allowed to have a dual identity, independently managed by himself (for his green identity) and an identity provider in a blue country. This requires legal provisions for service users from green Member States to acquire a second blue identity from any blue Member State, as well as being enrolled in all kinds of e-Identity support programs. It may also require legal provisions to be allowed to use self managed identities provided by a green country to users in blue countries.

The scope of this dual identity provision needs further study but could well include the consequence of providing dual (electronically readable / writable) identity documents, (e.g. passports3), tokens and or administrative provisions. Administratively these service users would be duplicated, with one instance managed in a blue Member State and the other instance self managed from a green Member State.

The acceptability of this solution will decrease as the number of service users benefiting from this approach increase. This can be easily understood by considering that from a statistical point of view the service user himself is the only one that knows the difference between himself as a service user with dual identities in green, resp. blue environment and two independent service users that only operate in either green and blue Member States, respectively. Providing selectively a dual identity thus creates a semantic aggregation conflict between users and their identity records. This conflict should be kept limited to a marginal problem. Whereas the deployment cost of this solution is relatively low, the indirect costs can potentially explode when usage grows beyond a negligible percentage.

6.2. Dual identity handling by service providers

Instead of administratively duplicating the service user a duplicated service provider interface could be implemented. Each Member State would implement dual versions of each relevant service that would need to be accessed by either service users from blue and green Member States, respectively.

The problem with this solution approach is that it highly depends on the nature of the service what the impact is of this approach. In a minimal case, where the service itself does not involve any personalized information of the service user, for example, when the only identification objective is to let the user pay for the service, it can be adequate to just have a duplicated service portal for green and blue environments, respectively, whereas the service behind the portal is shared. But in other cases, that more deeply involve service user identity related activities, several other components of the service may need to be duplicated. In the worst case the entire service has to be duplicated, and back-end integration between the two service versions is necessary.

The problem is that this kind of solution depends on the degree of duplication required. In a minimum scenario (only duplicate service portals) a small additional cost for implementing and maintaining a separate portal for service users of the other color is the only consequence. In the other extreme, services may have to be re-engineered in order to be able to support dual blue and green identity management schemes. In contrast with the dual identity approach this approach is more feasible when a significant number of cross over service users needs to be accommodated.

A second type of problem that can occur is the risk of unavoidable semantic integrity conflicts, in particular when a fraudulent scheme could be setup using (fake) dual identities from green and blue Member States. For each individual service a careful analysis is required before a duplication for green and blue environments can be implemented.

The cost profile of this solution is characterized by a high initial cost, that scales linearly with the services being provided, and running costs after deployment that are relatively small, and not dependent on scale.

6.3. Ignoring the semantic conflict with backup in legislation

A third way to address the conflicting blue and green identity management scheme is by technically
ignoring it, and providing backup by legislation. In this case parallel green and blue e-Identity spaces would exist which are unconnected in the virtual world. The only bridging would be in the real world. This would work as follows:

1. Legislation will be implemented that defines that in all circumstances service users from a green Member State are protected by green legislation, also when obtaining services from a blue service provider.
2. Similar legislation will be implemented that defines that in all circumstances service users from a blue Member State are protected by blue legislation, even when obtaining green services.
3. The service providers technically implement a blue or green solution in line with their national policies and legislation, and are prepared to handle manual corrections whenever issues arise with a service user from a Member State of the other color.

Like in the first case, this approach can only be acceptable when it applies to a limited number of cross-color cases. Even when only a few percent of service users obtain services from a cross-color service provider, we may assume that even then the majority of cases does not raise issues.

The complexity of this approach is that a sufficiently homogeneous legislation within both the group of blue Member States and within the group of green Member States is assumed. In detail this assumption is not entirely correct, and therefore implementation of this approach is likely to require complex and time consuming negotiations both in the group of blue and the group of green Member States. An overview of the main advantages and disadvantages of the proposed solutions are summarized in

Table 1. The research program of the STORK project will make a more in depth assessment of these strengths and weaknesses of each approach.

<table>
<thead>
<tr>
<th>Evaluation criteria</th>
<th>Dual identity</th>
<th>Dual provision</th>
<th>Legal cover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislative overhead</td>
<td>Only initial</td>
<td>Only initial</td>
<td>Both initial and continuous</td>
</tr>
<tr>
<td>Scalability</td>
<td>Restricted to low volume</td>
<td>Yes</td>
<td>Restricted to low volume</td>
</tr>
<tr>
<td>Dual passports, tokens, etc</td>
<td>Probably required</td>
<td>Not necessary</td>
<td>Not necessary</td>
</tr>
<tr>
<td>Service independence</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Fraud vulnerability</td>
<td>Service independant, potentially low</td>
<td>Service dependant, potentially high</td>
<td>Service independant, potentially high</td>
</tr>
<tr>
<td>Demographic pollution</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Service integrity</td>
<td>Not impacted</td>
<td>Service dependant</td>
<td>Service dependant</td>
</tr>
</tbody>
</table>

7. Conclusions and research directions

The STORK project aims at implementing an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State. It will also pilot cross-border e-Government identity services and learn from practice on how to roll out such services, and to experience what benefits and challenges an EU wide interoperability system for recognition of eID will bring.

The STORK interoperable solution for electronic identity (eID) will be based on a distributed architecture that will pave the way towards full integration of EU e-Services while taking into account specifications and infrastructures currently existing in EU Member States. The solution provided is intended to be robust, transparent, safe to use and scalable, and should be implemented in such a way that it is sustainable beyond the life of the pilot.

The STORK project will:

- Develop common rules and specifications to assist mutual recognition of eIDs across national borders;
- Test, in real life environments, secure and easy-to-use eID solutions for citizens and businesses
- Interact with other EU initiatives to maximize the usefulness of eID services.
It will do so by preparing for and implementing several pilots with services that will have significant potential impact and are adequately secure, by making use of open standards where possible and respecting with data protection regulations. The pilots will test the common specification on eID for several applications that have a substantial impact on e-Government across Europe.

The interoperability solutions discussed in this paper will be used as templates for real implementation.

8. References


