Raising Acceptance of Cross-Border eID Federation by Value Alignment

Jérôme Brugger, Marianne Fraefel and Reinhard Riedl
E-Government Institute, Berne University of Applied Sciences, Berne, Switzerland
jerome.brugger@bfh.ch
marianne.fraefel@bfh.ch
reinhard.riedl@bfh.ch

Abstract: A common identification and authentication space is one of the goals set in Europe's Digital Agenda. Interoperability of electronic identities (eIDs) across Europe will facilitate mobility and cross-border e-business and therefore contribute to growth. Large Scale Pilots STORK and STORK 2.0 have designed a technical solution and are developing a model for offering cross-border eID use as service. A major challenge remains in growing acceptance for such a system by end users, service providers and national governments alike. This paper examines the different aspects influencing the long-term success of European identity federation, which enables cross-border eID use for accessing e-government and private services. A special emphasis is put on the value perspectives of the individual stakeholders and the public value assessment of the solution. Based on a literature review, it offers a framework for analysing acceptance criteria according to different stakeholder groups (governments, service providers, end users). It takes into account the trust component, the mutual influence of acceptance decisions and the importance of contextual factors influencing the actors' choices. The discussion is based on a reflection of existing conceptual approaches in the field of technology acceptance in general and eID development in particular and draws on preliminary empirical data from the STORK 2.0 project. The paper outlines the challenges of creating a European interoperability solution, which allows a convergence with the development of national eID strategies and fits the value expectations of all stakeholders. In an organizational perspective, it touches upon requirements for creating an identity ecosystem with a network character but centralized services and decisions. In conclusion, the paper presents critical success factors for advanced collaboration between private service providers and government agencies across Europe on the subject of eID development. Thereby it assesses the current status of realization and outlines the challenges and opportunities ahead.

Keywords: electronic identification, federated identity, technology acceptance, large scale project, multi-stakeholder coordination, public value

1 Introduction

Electronic identities (eIDs) are one of the key technologies to deliver better e-Government services at lower costs. EIDs allow fully electronic transactions with secure, proven and legally valid identity information and thereby enable seamless digital processes, eliminating any paper based signatures or personal appearance for identity check. Besides the use in e-government applications, eID may help private service providers to lower their identity and access management costs. The current use, restricted to the national context in which the eIDs are issued, is a serious limitation to value creation. In the Digital Agenda 2020 the European Commission (EC) has set the goal to create a digital single market for Europe enabled by a single identity space. The approach to deal with the current heterogeneity of eIDs is to foster interoperability of the national systems. This requires an interoperability layer, which hides the complexity of the different systems in technical and organisational terms and allows user-controlled transactions of identity credentials between a user from country A and a service provider from country B.

On the policy side, a new "Regulation on Electronic Identity and Signature (eIDAS)" has been adopted in July 2014. EIDAS provides the legal framework for cross-national identity federation and thereby certainty on the cornerstones of future development for all stakeholders involved. It covers the general terms of mutual acceptance of national eIDs in the area of e-Government under well-defined conditions. However, the regulation leaves it open to every Member State (MS) whether to join the mutual acceptance regime or not by notifying their national eID solution. This approach is asking for additional efforts in order to achieve maximal coverage across Europe, since national states need to actively participate in the mutual acceptance scheme. Furthermore, some of the essential details are still unknown. The implementing acts are currently being drafted by an expert group and will regulate the exact procedures of the trust model. In addition to eIDAS, the European Service Directive is demanding MSs to set up an e-government single point of contact for businesses

Reference this paper as Brugger J, Fraefel M and Riedl R. " Raising Acceptance of Cross-Border eID Federation by Value Alignment" *Electronic Journal of e-Government Volume 12 Issue 2 2014, (pp179-189)*, available online at www.ejeg.com

source: https://doi.org/10.24451/arbor.7723 | downloaded: 27.7.2024

from other European states. The full potential of this service will only be reached, if all business to government transactions can be done online, using a foreign eID to authenticate to e-government portals.

For the purpose of developing the infrastructure for cross-border interoperability, the European Commission (EC) has set up several so-called Large Scale Pilots (LSPs). One of them is the project "Secure idenTity acrOss boRders linked" (STORK), which ran 2008-2011. It was co-funded by the EC as part of its Competitiveness and Innovation Programme (CIP) and was implemented by a consortium of 35 partners from 18 EU member states and associated countries. STORK developed common specifications to assist mutual recognition of eIDs across national borders. The interoperability specification was tested in six e-Government pilot applications (STORK, 2012).

The follow-up LSP, STORK 2.0, is again co-funded by the EC. It is implemented by a consortium of 58 partners, comprising 19 EU member states and associated countries (13 of them were already involved in STORK) and will run 2012-2015. STORK 2.0 builds up on the results of STORK by developing and testing common specifications and building blocks for the interoperation of eID for legal persons' identities and the facility to mandate on top of the existing solution. STORK 2.0 demonstrates interoperable services in real-life settings based on pilots (e-learning and academic qualifications, e-banking, public services for business, e-health). The four new pilots widen the market perspective by addressing new sectors within and beyond e-government.

While the technical solution (cf. Leitold and Zwattendorfer, 2011) is in place and is currently being enhanced, the main challenge lies in raising acceptance for the cross-border use of eID within the federation. STORK 2.0 deals with this issue by exploring requirements for sustainability. They include packaging cross-national authentication as a service for governments and businesses, developing a cost model and promoting the service (cf. STORK 2.0, 2013a). Corresponding measures should also impact the usage of national eIDs, which has not reached its potential of being the standard authentication method for secure transactions in most of the countries. Cross-border applications increase the value for eID owners, while at the same time relying service providers can accept multiple eIDs through one interface.

This paper aims at analysing acceptance factors that are relevant to the different stakeholders and contributes a framework for examining interdependencies of acceptance criteria. The specific stakeholder view needs to be completed with an overarching view on value creation, in order to identify a possible convergence of public and private stakeholders' value perceptions. This allows widening the view form a specific interoperability solution to a holistic approach of a European e-identity ecosystem.

The paper is structured as follows: Section two provides a literature overview aimed at identifying relevant adoption criteria for the up-take of eIDs, eID systems and cross-national identity federation. By including the public value concept, the section seeks to link research on eID adoption with considerations on formulating adaptation strategies in a multi-stakeholder context. Section three presents a framework, which structures the main acceptance factors for different stakeholder groups and sets out the methodological approach. In section four the different stakeholders and their acceptance behaviour are analysed based on empirical findings delivered in the STORK 2.0 project. In section five, the main interdependencies are summarized, followed by the conclusions in section six.

2 Literature discussion

The question of how a European identity space can be established touches upon a range of research fields within and beyond e-Government. First, theoretical approaches aimed at explaining the diffusion of innovations at large and the acceptance of information systems in particular provide a starting point for structuring influential factors relevant to the present case. Second, the development of a cross-national eID infrastructure can be reflected in the light of conceptual approaches from research on e-Government development, including issues such as infrastructure development, interoperability, concept and benefits of identity federation and differences in the value assessment of e-Government systems by the public and the private sector). Third, the concept of public value helps developing an overarching perspective, pointing at the need for common goals when establishing public-private cooperation. Fourth, empirical findings on the actual state of eID diffusion, including take-up by governments and end users set a frame for the discussion on the future development of cross-national identity federation.

2.1 Theoretical approaches on technology acceptance and diffusion

The diffusion of innovation (DOI) theory (Rogers, 2003) proposes a five-stage model of diffusion. From an individual actor's point of view, five perceived attributes of the innovation are considered as relevant in the decision stage: "*relative advantage* (comparing the innovation with the previous solution); *compatibility* (consistency with existing values and needs); *complexity* (difficulties in understanding and using); *triability* (possibility to experiment with); and *observability* (visibility of innovation results)" (Aichholzer and Strauss, 2009: 232). The named factors can be applied to any type of innovation, including information systems, and to individuals and organizations alike.

The technology of acceptance models (TAM) (Davis, Bagozzi and Warshaw, 1989) and its follow-up models such as TAM2 and TAM3 or UTAUT and adapted models (Venkatesh and Bala, 2008; Loo, Yeow and Chong, 2009) focus on the adoption of information systems in particular. Such models propose that the acceptance is determined by *perceived usefulness* (usage enhances performance) and *perceived ease of use* (usage is free of effort). Both factors bear resemblances to the assumptions formulated by the DOI theory. TAM has been operationalized with changing sub-variables for empirically testing the adoption of specific IT systems by individuals. Several factors that may influence technology perception relate to the concept of trust (Lee, Kim and Ahn 2011).
Trust relationships are essential for collaboration in electronic environments and may relate to different domains: On the technology side trust relates to *information* (quality) and *information systems* (security and reliability). On the actor side it relates to the *participants* in electronic transactions (e.g. consciousness of privacy and security issues). The following factors influence trust: *perceived trustworthiness* (expectations on competence, credibility, positive intentions, predictability, reliability etc.), *propensity to trust* (personality), *context* (situational factors) and *social trust* (trust of others) (Chopra and Wallace, 2003). As opposed to general adoption models, the concept of trust does not only focus on expectations towards technology as such, but integrates user expectations towards other actors and puts a stronger focus on contextual factors. Similar to the DOI theory it assumes that adoption (trust) by others is relevant for fostering the diffusion process.

2.2 Influence of contextual factors on the up-take of eID systems

Research in eID diffusion often refers to one or a combination of the above-mentioned theoretical approaches, while drawing on additional concepts that provide explanatory power in the field of e-Government. In their assessment of the development of the Austrian eID system, Aichholzer and Strauss (2009) build up on the *institutional actor theory* for modelling the interplay of social and technical factors in technology development, emphasizing the institutional context that shapes actors' choices. Regarding national eID systems, the following context factors are considered to influence the perceptions and strategies of stakeholders: *Legal regulations, political institutions and culture, economic institutions and market structures, socio-cultural structures* and, *technological pool*. The cross-national analysis of the development of eID systems in Europe by Kubicek and Noack (2010) complements this approach with the concept of *path dependency*. They find that besides cultural differences in the perception of the role of the state, previous technical, organisational and regulatory settings explain for the differences in the provisioning of national eID systems and thus the heterogeneous landscape of solutions and usage across Europe. Both approaches highlight that the broader situation needs to be reflected when assessing different stakeholders' decisions on the take up of eID solutions.

In the context of eID we can differentiate between three main stakeholder groups: governments responsible for the eID infrastructure, public and private service providers that implement authentication based on the eID and end users that use an eID to access a service. Up to now, research mainly focuses on public administrations and/or citizens as end users of an eID system. Private service providers are however an important stakeholder group when seeking to build up a European digital single market, for which cross-national identity federation is considered as a prerequisite.

In an earlier work on identity federation in Europe, Seltsikas (2005) provides a categorization of drivers that allow different stakeholders to address their needs: For the European Commission, economic strategies, the implementation of e-Government Directives and enabling new applications are considered the main drivers. Member states share these drivers while also being concerned with securing existing applications and keeping established legacy in place through integration/interoperability as well as with enhancing security, increasing

the take-up of online services and reducing costs. Fraud reduction and transaction convenience are considered the main issues for European citizens and businesses, while for the latter, the reduction of costs is also a main driver. As for the benefits of identity federation through an intermediary, Walser et al. (2013) point to *incentive-contribution problems*. In a situation, in which various parties are involved it is not apparent who profits from and who bears the burden of federated identity management, especially since the present costs for identity and access management are usually unknown – be it in the public or the private sector. The main benefit of an interoperability layer lies in the reduction of transaction costs through reducing the number of interfaces between partners, while expanding the number of stakeholders that use the infrastructure. The provision of an interoperability solution for identity federation shares challenges common to the development of new e-Government infrastructures (cf. e.g. Janssen, Chun and Gil-Garcia, 2009). This concerns the question of how collaboration of different stakeholders is established in an evolving system that can't be centrally managed. Furthermore, infrastructures typically need a critical mass of users to take off while bearing high investment costs. It is therefore important to have a closer look at the interdependencies between take-up decisions by the different actors involved. In the case of cross-national identity federation, these include different solution providers (eID systems, interoperability layer) and information providers (identity and attribute information). Provisioning of a cross-national authentication service will have to adequately reflect current business-models of all partners involved.

2.3 Public value research

The concept of public value was first used to describe strategy development for public administration (cf. Moore 1995). It introduces the triangle of *public value*, *sources of legitimacy and support* and *operational capabilities* and suggests that public administrations should address all three dimensions when developing a strategy . As Moore and Khagram propose, this triangle can also be made fruitful for businesses, when thinking about value creation beyond customers and stakeholders. This is especially true for businesses in a politicized environment (Moore and Khagram 2004). We suggest that the public awareness for privacy and data security makes the business related to all aspects of identity federation highly dependent on legitimacy which is supported by the public value of the solution. This needs to be considered as essential secondary factor for all stakeholders' decisions.

As research on the introduction of other e-government systems shows, the value attributed to the implementation and usage of an IT innovation is likely to differ between public and private stakeholders due to considerably differing needs and requirements (Raus, Liu and Kipp, 2010). Raus et al. propose a framework for assessing the perceived value on the following dimensions: *strategic, operational, social* and *financial*. As they point out, understanding value perceptions of all stakeholder groups is vital for supporting the diffusion process. For governments, long-term impact, incremental (rather than radical) change, and multiple forms and levels of public value incurred are very important for successful innovations (Dawes, 2013). In the context of identity federation, the networked character of the solution makes the interconnection of value perception by the different stakeholder a central factor, moreover the overarching view on the whole solution needs also to be taken into account.

2.4 Current state of eID up-take and diffusion

Current research on eID diffusion includes a range of country reports and some comparative analyses (cf. Kubicek and Noack, 2010). EU e-Government benchmarks provide empirical insights to implementation and usage of national eID systems in Europe. In 2014 two third of the assessed European and associated countries reported to have an eID system in place (Capgemini et al., 2014:67). Previous benchmark includes reasons to success or to failure regarding the implementation of an eID solution. The countries stated that the ease of use, low acquisition costs, and multiple usage possibilities are essential. Furthermore, the collaboration with the private sector and the level of security and trust are considered to be crucial for success. On the other hand, high costs, lack of supportive legislation and the complexity of the technology are some of the main barriers (Capgemini et al., 2010:119). Again, the current report shows, actual usage in selected services is lower than the general availability of the eID functionality. In 59% of some selected governmental services users could authenticate online, in 46% they could use a national eID (Capgemini et al., 2012: 51). This illustrates the gap between the technical realisation of eID systems and their success in terms of usage by governmental service providers. When looking at end users, research shows that the state of roll-out of a national eID may differ considerably across countries. Kubicek and Noack (2010) confirm that it is primarily the

costs and complexity of a given solution, which influence take-up and usage by citizens. On top, alternative authentication methods may negatively shape end users perception of the value of (generally safer) eIDs.
To sum up, the literature provides a fruitful basis for a discussion of adoption factors relevant for the development and diffusion of national eIDs and for addressing interoperability issues. Generic acceptance models are useful for discussing the technology assessment by single stakeholders. However, they insufficiently reflect the mutual influence of actual and expected behaviour by the actors involved. Also, they tend to neglect the structural opportunities and restrictions that influence stakeholders' decisions on the up-take of a given solution. In the context of identity federation, the concept of trust not only helps to fill in this gap, but is also inherent to according solutions, since federated identity management relies on trusting identity information provided by others. As for the stakeholders involved, private service providers as adopters of national or cross-national eID systems are underrepresented in current research discussions. The present article contributes to filling in this gap by referring to the public value concept.

3 Conceptual approach and methodology

Based on the discussion above, we select a set of criteria, which fit the main stakeholder groups, namely governments, private service providers and end users on an abstracted level. The proposed basic framework integrates contextual factors that may limit the options for decisions by the named stakeholders, especially while looking at governmental actors.

3.1 Framework for analysing acceptance of cross-national identity federation

Establishing a European identity space requires technology acceptance of different components by several stakeholders. Thereby we can distinguish between technology acceptance on the *national* and the *cross-national* level. On the *national level*, technology diffusion addresses the *end users* that are provided with or acquire a governmentally accepted eID and *public or private service providers* that implement the authentication service based on the eID solution. On the *cross-national* level, member states and associated countries need to connect their national eID infrastructure to the *interoperability layer* provided by STORK. Furthermore, public and private service providers need to implement the *STORK authentication service* into their platforms so that identity information can be received from a given national eID provider. End users will have to accept the authentication solution and allow the transfer of their credentials to national and foreign service providers when engaging in online transactions.

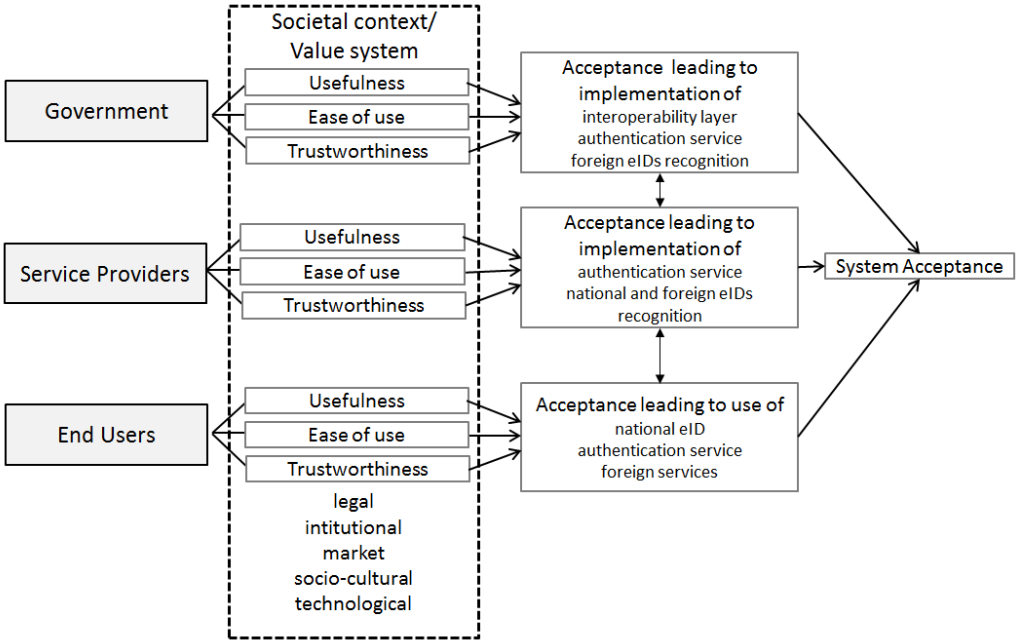

Figure 1: Stakeholder and system acceptance framework

The conceptual approach on acceptance takes into account the *contextual factors* moderating the perception of usefulness in terms of value to the stakeholder, the ease of use and the perception of trustworthiness of the system components and the transferred information, i.e. the *acceptance factors*. Since the perception of

usefulness will not only depend on a stakeholders' current situation, but also on the expected decisions and actions of the other stakeholders, the mutual influence among acceptance decisions is included in the framework.

3.2 Empirical basis

In the following section we focus on conceptual issues of acceptance in a complex system and support these findings with qualitative and quantitative preliminary results from the STORK 2.0 project. Four sources of data are used:

- *Service provider interviews* provide insights to the perception of the service by business and technical decision makers from four defined sectors (banking, health, academic, and telecommunication) (STORK 2.0 2013b).
- An *end user survey* assesses current and intended use of eIDs (STORK 2013b, Appendix 11).
- A *questionnaire on business plans* answered by *country representatives* surveys the current situation and the future development plans for the national eID systems for the next 3-5 years (STORK 2014b).
- In addition to the empirical findings from the project activities, 14 *European CIOs* or representatives of the CIO office were interviewed on the challenges and futures plans on eID in national and cross-border perspective.

4 Acceptance by stakeholders

Based on the results of the project and the specific situation in the STORK 2.0 environment, adoption criteria and contextual influences will be examined for the main stakeholder groups involved. Their perspective on the value of the service and their main requirements towards it lay the grounds for further considerations on the acceptance of the service as a whole.

4.1 Governmental stakeholders

Bearing in mind the different roles governments fulfil in an eID federation (running a national eID system, offering e-Government services relying on the eID, setting the legal framework), we focus on two main points: the fit between national eID strategies and European regulation and the usefulness of the service in different value perspectives.

4.1.1 Contextual factors

The development of national eID systems is a precondition for establishing a European interoperability solution. The CIO interviews confirmed that this tight link makes building up a national system the first priority for governments. However, in many cases the national eID system has not yet reached a high maturity, some are still under development or major changes are impending. Raising take-up of the national solution is still a major concern in most countries. In this perspective, the question of strategy fit between the European policy and the country situation is one major issue influencing further decisions on actions. The national solutions differ in

- the level of quality (defined in the quality assurance levels (QAA) of STORK), taking into account the technical solution and the issuing and delivery process,
- the pricing applied. Most countries charge for the eID token, while only in a few cases transactions are charged.

Both issues need to be aligned on a European level, but a proper assessment of the strategy fit has not been achieved yet, since the decisive legal framework on the European level has just been recently passed and the details (the implementing acts to the eIDAS Regulation) are not know yet. In CIO interviews, the forthcoming regulation had been confirmed to be the major source of uncertainty leading to a situation, in which decisions are postponed. The eagerly expected clarification will now help governments to adjust their future plans to the European regulatory actions on interoperability.

4.1.2 Acceptance factors

There is little empirical data on the perceived value of the European solution. The increasing participation of member states (MS) in STORK 2.0 can be seen as a confirmation of their positive perception. In the business plan survey, countries reported heterogeneous priorities for implementing cross-border authentication in e-

government services. The pilot cases in STORK 2.0 indicate potential priorities in higher education and healthcare. But given that not all MS participate in every pilot, these priorities are not commonly shared. In the same survey, no clear priorities on which private services should be targeted for the use of cross-border eID were reported (STORK 2014b). This illustrates, that there is no shared understanding on which sectors will want to benefit from cross border eID use.
STORK 2.0 has developed a list of six factors to assess the value generated. Besides direct and indirect financial gains, the solution will help to achieve cybersecurity gains, societal gains, policy gains and macroeconomic gains (STORK 2.0, 2014c). Policy gains and macroeconomic gain have been at the centre of the argumentation for a digital single market. Assessing the public value on a conceptual basis points on one hand towards the value an optimized process has for the administration itself, leading to more efficient and cheaper public administration. On the other hand, the increase of trust in electronic transactions and the cross-border use of trust services serve the public value of the solution. Since security, trust and privacy issues are not only a potential threat to functioning e-government solutions but also to any kind of private electronic services, the emphasis of the public value can help to legitimize the investments needed and to strengthen business engagement for the solution.
Up to now, the value discussion has not been fully translated into a national perspective, e.g. by formulating measurable goals. The political decision, whether the national solution should be notified under the eIDAS regulation will be a catalyser for this, but the effects are not visible yet. Since governments are confronted with potential costs, a solid evaluation on the value generated is urgently needed. Based on the requirements towards the support organisation, MS will have to invest in own activities or contribute to a central organisation. Either way, the countries connected to the interoperability layer will have to contribute resources (STORK 2.0 2014a).

4.2 Service providers

Service Providers rely on the identity information coming from the electronic identity system to grant access to their system. In this section we are focussing on private service providers, which would, by adopting the solution, help to deliver actual value to end users.

4.2.1 Contextual factors

The contextual factors influencing the perception of the system mainly consist of the market situation and the technological pool in terms of alternatives for authentication, the legal framework (compliance with national regulations) and the societal attitude towards eID systems as manifested in the current take-up and usage numbers.

4.2.2 Acceptance factors

From a conceptual point of view, the value service providers will get from the interoperability infrastructure consist of

- a reduction of costs for identity and access management, since they can rely on federation.
- an increase of their potential customer base without additional complexity.

The empirical data on the attitude of service providers is limited four sectors, but shows a generally positive attitude towards the service as it was presented to them in the panels, indicating that at least some of the benefits are well perceived. Business oriented participants rated the quality assurance levels (QAA) the most important service feature, indicating the importance of trustworthiness. The QAA are the instrument developed within STORK to map eIDs to one of four defined quality levels. Given the heterogeneity of national eIDs, service providers can define a minimal level of quality needed to access their service. Service design considerations show, that the trust in other national solutions can be assured by applying and maintaining the instrument of quality assurance levels. The open question herby is how the current system of self-assessment could be improved without creating substantial additional burden or limiting the countries' sovereignty. Further important factors are the user coverage, the availability of sample services and promotional activities, thus pointing to the impact of acceptance by other stakeholder groups. Thirdly, the user interface is perceived as important. This feature implies that the interoperability solution must blend into the user experience of a given service. Thus, consistency with the own system is important for service providers. Representatives of the technical side emphasized the importance of the API, developer manuals, the customer service and the test environment. This shows that adoption decisions will rely on the ease of use and the ease of implementation from the technical side (STORK 2014a).

Furthermore, the reliability of the interoperability layer is of concern. The infrastructure itself must be trusted by the service providers. Currently, the infrastructure comes with the logic of governmental infrastructure at best effort. Private service providers are used to rely on services at defined service levels, assured by contractual agreements. This basic difference between the public and private service provider way of functioning will be solved by the eIDAS Regulation by defining liability of the service. The general perception of the service by potential service provider has shown to be positive according to the interviews carried out in the project. Nevertheless, the question financial gains by process optimization, reduction of fraud and larger base of potential customers and the corresponding costs for implementing and maintaining the STORK 2.0 solution need credible and concrete answers. During the pilot phase of STORK 2.0, figures regarding these questions will be surveyed.

The contribution of service provider to the public value of the solution could be used as an additional argument for service providers: Not supporting the solution augments the risk of a general loss of trust in electronic solutions, which may impact their business and internet services as such. Again, this negative impact would impact the public value of the solution. Positively spoken, aligning the business goals of a private service provider with a contribution to the development of European trusted identity infrastructure does offer additional benefit to service providers in terms of legitimation for their use of identity data and the long-term trustworthiness of electronic services.

4.3 End Users

4.3.1 Contextual factors

The influence of contextual factors on the adoption decision by end users has not yet been extensively studied in the end user survey. We assume, that privacy and security guaranteed by a legal framework, alternative solutions and the social acceptance of the eID solution will have a high impact.

4.3.2 Acceptance factors

The value attributed to the service will be derived from its usefulness which is based on the services offering cross-border eID authentication. End users indicate four main reasons preventing them from eID use (STORK 2.0 2013):

- high price
- high complexity
- obstacles for acquiring an eID
- the lack of trust in the solution

These issues must be mainly solved in the national solutions, but are also impacting the interoperability layer: The complexity of the solution must be completely hidden from the end users while fostering trust at the same time. Simplicity and user-friendliness of the user interface are one key to grow trust. Acceptance by end users will be firstly influenced by the familiarity with eID based on national usage. Secondly, the service offered by the service providers shape end users behaviour and thirdly, the public value of the solution in terms of the societal benefits from the solution may again be secondary criteria for acceptance.

5 Mutual influences of acceptance and success factors

A range of adoption factors from the view of the different stakeholders have been discussed. The success of the overarching interoperability system will lie in a convergence of the different perceptions of its usefulness and value. In the following section we discuss positive and negative mutual influences between the different stakeholders.

5.1 Business model and cost share

The sharing of costs and benefits among the different stakeholders is a major challenge, which lies ahead. In addition to the costs of the national eID systems, governments are facing costs for the interoperability infrastructure: Costs to run the actual infrastructure and costs for delivery, support and maintenance of the system. Provisioning extensive support will ensure the connection between service providers and the interoperability layer. Additionally, service providers will also have to respond to end user support requests, for which second level support must be provided. The organisational options to assure support have been

drafted, an efficient provisioning of support throughout all connected national systems will require centrally organized actions but at the same time local contact points in order to assist customers in local language, which might be tied to the support organisation for the national eID solution. In addition, pro-active and re-active audits and possibly some cyber security surveillance create additional costs, all of which heavily depend on the implementing acts to the eIDAS Regulation. Currently, there are no cost estimates since no decision on the organisation has been taken.

The main financial benefits of the interoperability solution will be obtained by service providers, both private and public. Given the lack of well-grounded assumptions on the type and number of services that will use the interoperability solution, the benefit of the solution cannot be properly estimated. At the same time, the revenue perspective is still unclear, since it will be influenced by the eIDAS Regulation. The strategic and financial value of a European identity space is still an abstract concept. The uncertainty on the actual running costs for such a solution limits the possibilities for a clear commitment by governments, which would be an important signal to private service providers.

5.2 Trustworthiness

Trustworthiness of the solution is essential in the context of identity federation. End users and service providers alike make their decision depending on the perception of trustworthiness. Governments in their role as service providers depend on mechanisms assuring trust and reliability of the solution themselves. Governments are at the same time responsible for providing the legal, technical and organisational framework to foster trust in the solution. Thereby, it seems that governments are inclined to limit their liability and offer the service at best effort, which does not meet the private service providers' usual criteria for buying into a given service.

STORK 2.0 is exploring further possibilities of standardisation and the potential need for a neutral accreditation body. Accreditation of the different participants and components of the interoperability system could provide the necessary trust for service providers and end users. Organisational enhancement of the trust relationships on the other hand leads to a more complex structure less easy to implement. The different expectations towards the trust components of the interoperability framework remain one of the central challenges within the project.

5.3 Value alignment

On an abstract level we can observe that the commercial and political value stakeholders will attribute to the solution goes together with values the stakeholders will not primarily benefit from but have an important effect on the perception of the solution. We have used the concept of public value to describe these benefits, lying mainly in upholding the trustworthiness of electronic transactions in a general sense for all stakeholders. Up to now, the public value of the solution is a generic description, comparing eID federation to a modern infrastructure with benefits for all. Further research should be undertaken in order to attribute measurable elements to this value dimension. Interviews with stakeholder could also look into the question, which impact this value dimension has for take-up decisions and how this concept can be better used to link the different stakeholders' interest together.

5.4 Expected stakeholder behaviour

The central challenge pictured in the research framework is the mutual influence of acceptance decisions among stakeholders, relating to a chicken-and-egg problem. Securing the success of the interoperability platform will depend on the coverage in terms of countries, users and attributes. Positive signals, indicating raise of acceptance by the other group will influence the own decision. Government stakeholders have the biggest impact in this system, since they can influence both sides: they can promote the national eID and at the same time implement cross-border authentication in their own services. Coordinated priorities across the different countries will help to grow acceptance and demonstrate the reliability of the service.

6 Conclusion

Previous research has stressed the necessity of an appropriate design and a proper contextual embedding for the success of innovation. We have derived a simple model from existing literature in order to frame the specific case of a European eID federation and to address today's challenges and drivers for its realisation. Our

findings point to common needs among stakeholder groups, such as the high relevance of a clear QAA (quality assurance level) regime as well as to common problems, such as the unclear implications of the abstract concept of a digital single market. But the analysis also highlights that the needs and requirements of the different stakeholders – end users, governments and private service providers – may be conflicting in several key aspects. Since acceptance decisions of key stakeholders mutually depend on each other, this situation together with the unclear distribution of costs and benefits limits the likelihood of an economically driven self-organisation. As a consequence, decisive actions of national governments in favour of the interoperability solution are needed to enable the emergence of a rich and heavily used eID ecosystem. Currently, the contextual factors, namely the path dependency of the national eID strategies and the outstanding details to the European legal framework, hinder the development of a convergent value perspective for all stakeholders. Nevertheless, the decision process in each national state on notifying their eID solution forces the national governments to clarify their strategy. A firm decision to notify the solution and to subsequently implement cross-border authentication in e-government services will help to address the doubts of the other main stakeholder groups.

Ecosystem considerations, putting the public value perspective at its centre, can help to make the benefit for all stakeholders visible. Private service providers will base their acceptance decision firstly on clear assessment of the monetary gains, but the question of legitimacy for processing personal data can have a high impact on businesses as well. The public value perspective can be used to make the alignment of the value perspectives visible.

The framework applied in this paper provides a solid guideline for enhancing the heuristic approach adopted here. The operationalization of the framework for further quantitative research would allow for refining the mutual influences of adoption criteria in the context of eID development.

Acknowledgements

STORK 2.0 is an EU co-funded project INFSO-ICT-PSP-297263. STORK 2.0 consortium members provided input to these findings.

References

Aichholzer, G. and Strauss, S. (2009) "Understanding a Complex Innovation Process: Identity Management in Austrian E-Government", *Proceedings of the 10th Annual International Conference on Digital Government Research* (dg.o '09), pp 230-239.

Capgemini et. al. (2010). *Digitizing Public Services in Europe: Putting ambition into action. 9th Benchmark Measurement.* Report prepared for the European Commission[online] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=747.

Capgemini et al. (2014). Delivering the European Advantage? 'How European governments can and should benefit from innovative public services' – Final Background Report, [online], http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5812

Chopra, K. and; Wallace, W.A. (2002) "Trust in Electronic Environments", *Proceedings of the 36th Hawaii International Conference on System Sciences* (HICSS'03) [online] http://www.hicss.hawaii.edu/HICSS36/HICSSpapers/STFMS01.pdf.

Davis, F. D., Bagozzi, R. P. and Warshaw, P. R. (1989) "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," Management Science, Vol. 35, pp 982-1003.

Dawes, S. (2013) "Public Sector Knowledge Networks: Measures and Conditions for Success" in Gil-Garcia, J.-R. *eGovernment Success Factors and Measures: Theories, Concepts, and Methodologies*, Hershey: IG Global, pp. 88–103.

Janssen, M., Chun, S.A. and Gil-Garcia, J.R. (2009) "Building the next generation of digital government infrastructures", *Government Information Quarterly,* Nr.. 26, pp 233-237.

Kubicek, H. and Noack, T. (2010) "Different countries-different paths extended comparison of the introduction of eIDs in eight European countries", *Identity in the Information Society*, Vol. 3, No. 1, pp 235-245.

Lee, J., Kim, H.J. and Ahn, M.J. (2011) „The willingness of e-Government service adoption by business users: The role of offline service quality and trust in technology", *Government Information Quarterly*, Nr. 28, pp 222-230.

Leitold, H.and Zwattendorfer, B. (2011) "STORK: Architecture, Implementation and Pilots" in: Pohlmann, N.; Reimer, H. and Schneider, W. (eds.*), ISSE 2010 Securing Electronic Business Processes*, pp 131-142 [online] http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/1577/article.pdf?sequence=1

Loo, W.H., Yeow P.H.P. and Chong, S.C. (2009), "User acceptance of Malaysian government multipurpose smartcard applications", *Government Information Quarterly*, Nr. 26, pp 358–367.

Meynhardt, T. (2009) Public value inside: What is public value creation?, *Intl Journal of Public Administration*, 32(3-4), 192-219.

Moore, M. (1995) Creating public value : strategic management in government, Harvard University Press, Cambridge Mass.

Moore, M. H., and Khagram, S. (2004) "On creating public value. What Businesses Might Learn from Government about Strategic Management" Corporate Social Responsibility Initiative Working Paper No. 3, [online] http://www.hks.harvard.edu/m-rcbg/CSRI/publications/workingpaper_3_moore_khagram.pdf.

Raus, M., Liu, J., Kipp, A. (2010), "Evaluating IT innovations in a business-to-government context: A framework and its applications", *Government Information Quarterly*, Nr. 27, pp 122–133.

Rogers, E.M. (2003), *Diffusion of innovations*. 5th edition, Free Press, New York.

Seltsikas, P. (2005) "Can Europe's governments manage identity?", *BT Technology Journal*, Vol 23., Nr. 4, pp 80-88.

STORK (2012) "STORK – What is it?" [online], https://www.eid-stork.eu/index.php?option=com_content&task=view&id=37&Itemid=61

STORK 2.0 (2013a) "About the project" [online], https://www.eid-stork2.eu/index.php?option=com_content&view=article&id=15&Itemid=29.

STORK 2.0 (2013b): *D7.1. Consolidated Market Research* [online] https://www.eid-stork2.eu/index.php?option=com_jdownloads&Itemid=107&view=viewdownload&catid=4&cid=41

STORK 2.0 (2014a): *D7.2. Service Design* [online], https://www.eid-stork2.eu/index.php?option=com_jdownloads&Itemid=107&view=viewdownload&catid=9&cid=74

STORK 2.0 (2014b): *D7.3. Business Plans* [online], https://www.eid-stork2.eu/index.php?option=com_jdownloads&Itemid=107&view=viewdownload&catid=9&cid=75

STORK 2.0 (2014c): *D7.4. Sustainability Report and Recommendations* [online], *https://www.eid-stork2.eu/index.php?option=com_jdownloads&Itemid=107&view=viewdownload&catid=9&cid=76*

Venkatesh, V. and Bala, H. (2008), "Technology Acceptance Model 3 and a Research Agenda on Interventions", *Decision Sciences*, Vol. 39, Nr. 2, pp 273-315.

Walser, K., Brugger, J., Selzam, T. and Bernold, R. (2013) "Benefit model for distributed federated identity management in e-society using an intermediary", *Proceedings of the 7th International Conference on Methodologies, Technologies and Tools enabling e-Government*, (MeTTeG 2013), pp 209-218.