Arne Tauber, Bernd Zwattendorfer, Thomas Zefferer - "STORK: Pilot 4 Towards Cross-border Electronic Delivery" - Electronic Government and Electronic Participation - Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart, 2011, pp. 295-301

STORK: PILOT 4 - TOWARDS CROSS-BORDER ELECTRONIC DELIVERY

Arne Tauber[1], Bernd Zwattendorfer[2], Thomas Zefferer[3]

Abstract – The European Commission's goal of a single digital market emphasizes the importance of interoperability of ICT services. Therefore, the Commission has launched several large scale pilot projects to ease interoperability efforts. The aim of the large scale pilot STORK is to establish an interoperability framework for the mutual recognition of electronic identities within the European Union. STORK runs a number of pilot services to demonstrate its interoperability framework and applicability. In this paper, we discuss the objectives, architecture and achievements of the STORK e-Delivery pilot. Cross-border e-Delivery is a key aspect towards a European single digital market and deals with the secure, reliable, and trustworthy delivery of electronic documents across Member State boundaries. We discuss benefits as well as the value of this pilot by showing how citizens can authenticate and register at foreign e-Delivery portals and how public administrations can deliver documents to citizens registered at foreign portals. We also discuss a currently missing legal basis and further steps that are necessary to ensure sustainability of the current e-Delivery initiatives.

1. Introduction

To reap the economic and social benefits from a single European digital market, the European Commission (EC) has published the Digital Agenda 2010-2020 [1]. This strategy document outlines important actions to maximize the productivity, competitiveness and digital economic growth within the European Union (EU). The Agenda states that the key actions and pillars to reach these goals are common standards and interoperability between different isolated IT services. This step is also manifested by the EU Services Directive [2], which is currently being implemented by the individual Member States (MS).

The EC has launched several European large scale pilots (LSP) in order to foster interoperability efforts by allowing citizens and businesses to use their domestic e-Government infrastructures also abroad. The LSP SPOCS[4] [3] has been launched in 2009 and aims at building a second generation of points of single contact (PSC) to assist Member States with the implementation of the Services Directive. Two main areas of SPOCS are the provision of an interoperability layer and framework for the cross-border recognition of

[1] E-Government Innovation Center, 8010 Graz Inffeldgasse 16/a, Arne.Tauber@egiz.gv.at
[2] E-Government Innovation Center, 8010 Graz Inffeldgasse 16/a, Bernd.Zwattendorfer@egiz.gv.at
[3] E-Government Innovation Center, 8010 Graz Inffeldgasse 16/a, Thomas.Zefferer@egiz.gv.at
[4] Simple Procedures Online for Cross-border Services, see http://www.eu-spocs.eu

electronic documents (e-Documents) and the reliable cross-border exchange of electronic documents (e-Delivery). STORK[5] [4] is another LSP and has been launched in 2008 with the aim to provide an interoperability framework for the cross-border mutual recognition of electronic identities (eID). The STORK interoperability platform will enable citizens, businesses, and public administration to use their own national eIDs for secure and trustworthy transactions when accessing e-Government services in a foreign Member State. STORK consists of a consortium of 32 partners from 18 Member States and associated states, involving both the industry and the academic sector. The project runs six pilot applications that demonstrate the implementation and applicability of the interoperability layer at services being operational on national level. Especially relevant for this paper, the goal of Pilot 4 is to provide an interoperable framework for cross-border electronic delivery. E-Delivery deals with the secure and reliable delivery of electronic documents having the quality of registered mail in a traditional process. This is actually an important feature as many administrative procedures require governments and public agencies to send documents with a proof of receipt. In particular this applies to the justice sector.

The aim of this paper is to discuss the STORK e-Delivery pilot, its objectives, architecture, experiences, and relations to other international initiatives. We discuss the pilot's use cases in Section 2 of this paper. In Section 3 we show how these scenarios can be realized by relying on the STORK interoperability framework to authenticate foreign citizens and using a gateway-based approach to share documents between different e-Delivery systems. An overview of major pilot running aspects is given in Section 4. We discuss missing pieces and further required steps for a sustainable e-Delivery interoperability solution in Section 5. Finally, conclusions are drawn.

2. Goals of the Pilot

In the last years, governments, public administrations, and postal operators have put many Internet based e-Delivery systems in place. Popular examples are the Austrian Document Delivery System (DDS) [5], the Italian Posta Elettronica Certificata (PEC) [6], the German E-Postbrief and upcoming De-Mail system [7], the Estonia DigiDoc portal, or the Moja.posta.si service provided by the Slovenian Post. All systems provide a secure, trustworthy, and reliable communication infrastructure with the quality of postal registered mail. So far, all mentioned systems are operated on a national level and are only accessible to citizens of the same Member State (MS), i.e. only citizens of MS A can register with an e-Delivery provider of MS A.

The goal of the STORK e-Delivery pilot is to tackle interoperability issues of e-Delivery on several levels. To review the levels being addressed by the pilot in more detail, we start with *Level 1*, which allows citizens of MS B to authenticate at e-Delivery providers of MS A. This scenario enables senders (e.g. public administrations) to not only address domestic recipients but also foreign citizens that register with the domestic system. Besides authentication, e-Signatures play an important role in the context of e-Delivery. For instance, recipients may pick up deliveries and create a signed proof of receipt with their eID. Interoperability Level 1

[5] Secure idenTity acrOss boRders linKed, see https://www.eid-stork.eu

is realized by connecting national e-Delivery providers to the STORK authentication infrastructure. This gives citizens the opportunity to authenticate at foreign e-Delivery providers using their domestic authentication infrastructure. We discuss the approach, concepts, and architecture of the STORK authentication framework in more detail in the next section. We also show how we have extended the STORK authentication protocol to allow for the creation of basic electronic signatures being recognizable in a foreign MS.

Besides *Level 1*, the STORK e-Delivery pilot has further defined interoperability *Level 2*. Level 2 describes the use case of allowing citizens being registered with an e-Delivery system of MS A to deliver a document to a citizen being registered with a system residing in MS B. By combining this scenario with interoperability Level 1, a document could even be delivered to a recipient of MS C being registered with a system in MS B. Hence, Level 2 describes the real cross-border exchange of electronic documents between different MS. The main goal is not to realize this scenario between two systems only. We strive for the implementation of a scalable interoperability framework that allows for exchanging documents between arbitrary Member States. We discuss our approach and its basic workflows, which tackle this challenge, in the next section.

3. Interoperability Architecture

In this section we describe the main components of the STORK interoperability framework. In the first sub-section we focus on the general interoperability architecture allowing citizens the secure access to foreign services using their national eID. Subsequently, the interoperability framework enabling cross-border e-Delivery implemented in pilot 4 will be described.

3.1 Authentication

At the very beginning of the project, two authentication models have been identified, which build the basis for the common STORK interoperability layer. The first model is more or less a proxy-based approach where each MS deploys a national gateway (PEPS – Pan-European Proxy Service). On the one hand this national gateway integrates the national identification and authentication infrastructure and on the other hand implements the interoperability protocol for the secure exchange of identification and authentication data across borders. In this model, the PEPS acts as intermediary between service providers and a citizens. In the cross-border context, all PEPSs of the different MSs have a special trust relationship amongst each other. Contrary, the so-called Middleware (MW) model provides a direct communication path between the authenticating user and the service provider. The main advantage of this approach is the possibility of end-to-end security compared to the PEPS model. A drawback, however, is that each eID token provided needs to be integrated and maintained in the middleware.

One objective of the STORK project is now to combine both models. That means, that e.g. a citizen whose country is actually supporting the PEPS model on domestic level can also authenticate at service providers in foreign countries that follow the MW approach. Let us assume a scenario, where a citizen (e.g. recipient) of MS B wants to authenticate at an e-Delivery service provider of MS A. In our model MS A is a Middleware country and MS B is a PEPS country. The authentication process can simply be described as follows. When accessing the e-Delivery service provider website of MS A, the citizen chooses to login with foreign credentials. The service provider redirects the citizen to the Middleware, which runs

in the domain of the service provider. The citizen chooses her home country, is then redirected to the MS B PEPS and authenticates with her own eID. Subsequently, the PEPS of MS B redirects the citizen together with her credentials back to the MS A Middleware, which forwards the credentials to the service provider. For details on the STORK architecture and the interoperability models we refer to [4].

An important feature to mention at this stage is the ability of creating citizens' signatures through the STORK protocol as digital signatures play an important role in the field of e-Delivery. For that, the STORK protocol has been enhanced to transport both signature creation requests and responses inside its protocol messages. Those signature creation messages are extracted either by the PEPS or MW which are responsible for invoking an appropriate signature creation module. Details on the integration of this signature functionality can be found in the STORK interface specification [8].

3.2 Cross-border Document Exchange

In this subsection we present our interoperability architecture and framework for the cross-border document exchange of electronic documents. First, we take a closer look at the concept of the e-Delivery gateway, which builds the basis of our architecture. Subsequently, we continue to discuss the coupling of e-Delivery systems by using the delivery gateway protocol.

3.2.1 Electronic Delivery Gateway

In a first step, we discuss the bilateral case between two Member States only. For our consideration we make use of the interoperability framework for Pan-European e-Government Services (PEGS) [9]. PEGS is aligned to the European Interoperability Framework (EIF) [10] and is a pragmatic model proposing a layered interoperability architecture. The PEGS framework introduces a gateway approach that allows for coupling two different systems by defining the following four interoperability layers (from top to bottom): *procedural*, *semantic*, *technical*, and *trivial*. Basically, a PEGS gateway can be seen as a transformation service that translates objects between two systems. Thus, we introduce the notion of a so-called electronic delivery gateway (EDG) for our purposes in the field of e-Delivery. The first task of an EDG on procedural level is the harmonization of different or incompatible business objects and e-Delivery processes, e.g. dealing with different deadlines and numbers of evidences (delivery confirmation, proof of receipt). The semantic layer transposes different meanings of e-Delivery objects based on compatible and aligned processes, e.g. with respect to evidences, authentication levels and electronic signatures. The technical layer converts different e-Delivery protocols from one domain to another one. For example, the technical layer may have to convert a SOAP-based e-Delivery protocol to the Internet e-mail protocol SMTP. The trivial layer defines the underlying network layer. Since all systems are deployed on the Internet, we assume it is the same for all, i.e. TCP/IP.

3.2.2 Delivery Gateway Protocol

Attempts to connect all EU Member States and even additional non-EU countries according to this approach would lead to an N-to-N gateway interconnection network. However, we strive for a simple multilateral solution. Thus, we introduce an additional intermediate layer as illustrated in Figure 1. This layer uses the so-called delivery gateway protocol (DGP) which is a SOAP (Simple Object Access Protocol -based XML protocol covering generic

aspects of e-Delivery systems. This protocol is capable of carrying elements of all national e-Delivery systems in a common and generic way. As discussed above, interoperability requires the alignment of common business objects and processes, the creation of taxonomies of such objects, the alignment of their semantics, and the harmonization of protocols. A detailed taxonomy of e-Delivery systems aligned to all interoperability layers is provided by [11]. This classification is based on a requirements analysis for e-Delivery systems [5] according to several security properties assessed in [12]. The DGP is heavily aligned to this classification.

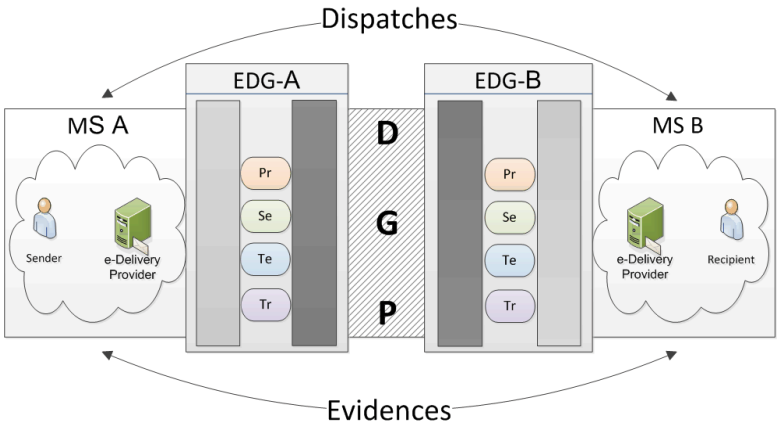

Figure 1: Electronic Delivery Gateway Architecture

As illustrated in Figure 1, the exchange of messages between two MS now requires two gateways. Consider the case where a sender of MS A wants to deliver a message to a recipient being registered in MS B. We assume that both gateways, EDG-A and EDG-B, are part of their respective domains. EDG-A translates the e-Delivery dispatch of MS A with respect to all interoperability layers to the DGP protocol. As both gateways are able to handle the DGP protocol, EDG-B can (re-)translate the DGP request to the e-Delivery protocol of MS B. The same procedure applies to evidences (delivery confirmations, proof of receipts). This is a very simplified illustration of cross-border document exchange. However, it demonstrates that MS A or B may be substituted by any other MS. This model thus allows us to bridge e-Delivery systems of any two MS.

Details of the cross-border e-Delivery gateway approach, also describing gateway interconnection, protocol details and trust establishment, are discussed in detail in [13].

4. Piloting

In order to demonstrate the applicability of the discussed interoperability framework, the STORK e-Delivery pilot has officially gone live in summer 2010 with an 18-month piloting phase running till end-2011. Four countries participate in this pilot: Austria, Estonia, Luxembourg and Slovenia. Finland has joined the pilot in a second phase in mid-2010. Luxembourg and Finland currently do not have any kind of national e-Delivery solution in place. Both countries participate in the pilot by connecting their STORK authentication infrastructure (PEPS) to the other countries' authentication infrastructure. This gives their citizens the opportunity to authenticate, register, and use all pilot services in the foreign country. Up to now, only the Austrian service provider has implemented the e-Signature feature so that recipients can create a proof of receipt by signing the message pick-up with a qualified electronic signature. Slovenia has implemented the signature feature at their PEPS.

Estonian and Finnish citizens can create the signature at the Austrian service provider (Middleware) using Java Applet technology. See [14] for more details on the approach of creating qualified electronic signatures using this technology.

Regarding interoperability *Level 2*, the pilot demonstrates the cross-border exchange of electronic documents between the Austrian service provider MeinBrief.at and the Slovenian service Mpstork.posta.si. Due to a missing legal framework, this interoperability level is only piloted for private sector deliveries. We discuss legal aspects in more detail in the next section. Cross-border document exchange between Austria and Slovenia is achieved by setting up two gateways. A central gateway has been set up in Austria serving Meinbrief.at (and all other Austrian e-Delivery providers as well). This gateway synchronously translates the Austrian e-Delivery protocol to the DGP and vice versa in real time. A second gateway is set up on the Slovenian side to translate messages from the Slovenian e-Delivery protocol to the DGP and vice versa. In contrast to the Austrian approach, this gateway does not directly deliver messages from Slovenian senders in real-time. Slovenian senders have to deliver messages to a particular mailbox of mpstork.posta.si. The gateway is pulling them in regular intervals for cross-border delivery.

One major task of piloting is to gather as much feedback as possible from both end-users and service providers and to evaluate this information. This is done by collecting data through statistical log data, interviews with service providers, questionnaires and filled-out feedback forms by end-users. Since we are evaluating the STORK integration only, it is very important to distinguish between feedback that actually refers to STORK authentication components and feedback that relates to software parts of service providers.

To sum up what we have learned so far: on the service provider side the major problem was to deal with new foreign identity attributes. For example, if an e-Delivery system is designed to operate on a certain format of the national identification number, the system may be completely redesigned to recognize and process foreign identification numbers as well. The feedback from end-users was overall positive without facing any major issues or hurdles at all.

5. Outlook

The European eGovernment Action Plan 2011-2015 [15] lists several key actions and priorities to create open, flexible, and collaborative e-Government services for citizens in order to enhance the mobility within the European single market. Section 2.2.2 (Personal mobility) of the action plan explicitly states the importance of the

[…] development of interoperable services enabling citizens to communicate, perform transactions, and send and receive electronic documents and information to and from public administrations across the EU. These will allow for delivering secure cross-border exchange and safe storage of electronic information (eDelivery of documents and information) […].

The main focus of STORK is providing an interoperability framework for authentication. This also applies to the e-Delivery pilot that provides suitable means to authenticate senders and recipients at all stages of e-Delivery processes.

STORK is intended to end in December 2011. To ensure that the outcome and achievements become sustainable, the STORK e-Delivery pilot has continuously contributed to other

initiatives and LSPs dealing with e-Delivery. Work package 3 of the LSP SPOCS, which supports the implementation of the EU Services Directive, is currently working on the provision of a cross-border e-Delivery and e-Safe interoperability framework. The STORK e-Delivery pilot has contributed to SPOCS in two ways. First, SPOCS has taken up the main concepts of the *Level 2* approach. The STORK cross-border delivery gateway protocol was refined by adopting several elements from the European Telecommunications Standards Institute (ETSI) Registered E-mail [16] specification. SPOCS has also specified in detail a governance structure maintaining the central TSL and has extended and optimized addressing mechanisms based on the standard e-mail address format. A further contribution was the use of the STORK SAML protocol in SPOCS to uniquely identify and authenticate both senders and recipients. SPOCS will start its 1-year piloting phase in June 2011 to demonstrate its applicability and qualification for cross-border e-Delivery. Nevertheless, sustainability should be supported through the take-up and maintenance of developed solutions by some organization. Thus, SPOCS is tightly collaborating with the industry and contributing to ongoing standardization activities. The SPOCS e-Delivery protocol is going to be standardized by the ETSI specialist task force (STF) 402, which aims at extending the current REM standard to establish interoperability between e-Delivery systems operating on different technical protocols, organizational aspects, and governance structures (policies).

Even if the standardization of the gateway approach is a first step towards a common e-Delivery space in this heterogeneous ecosystem, a legal framework and long-term governance strategy is currently still missing. Official deliveries by public administrations are usually regulated by law. However, in most Member States laws only cover the domestic delivery and do not deal with cross-border e-Delivery. This also applies to the counterpart paper mail. The only European reference for paper-based cross-border delivery of administrative documents is treaty °94 [17], dating back to 1977. However, this treaty was only ratified by eight European countries. Besides the legal basis, a proper governance structure is also important. Even if private sector systems could already be bridged using the introduced approach, this can only be achieved with a long-term governance structure in place.

6. Conclusions

Electronic delivery is mentioned in the European eGovernment Action Plan as key enabler for personal mobility of citizens throughout the EU. At the same time, the EC defines interoperability as one of the most significant key actions in the Digital Agenda towards a European single digital market. Pilot 4 of the EU LSP STORK tackles e-Delivery interoperability issues on several levels. Level 1 interoperability enables citizens to access foreign e-Delivery systems with their national eID by using the STORK authentication framework. Level 2 goes one step further and shows how real cross-border document exchange can be achieved by bridging different e-Delivery domains through a network and circle of trust between electronic delivery gateways. The pilot is currently in its running phase and demonstrates the applicability of the discussed architecture and concepts. In tight collaboration with the LSP SPOCS, the concept of real cross-border document exchange has been refined, enhanced, and optimized in a project environment dealing with e-Delivery to a larger extent. It is now important to ensure the sustainability of the developed solutions. In a first step this is achieved by standardizing the developed SPOCS cross-border e-Delivery protocol as an ETSI standard. However, to enable and establish e-Delivery interoperability on a European level, the EC is now asked to be on the spot to push on the creation of a legal basis on European level and the installation of an appropriate governance structure.

References

[1] European Commission: A Digital Agenda for Europe, COM(2010) 215 final/2, Brussels (2010)

[2] European Union: Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, Strasbourg (2006)

[3] Rössler, T., Tauber, A.: The SPOCS interoperability framework: interoperability of eDocuments and eDelivery systems taken as example. In: ISSE 2010 Securing Electronic Business Processes, 122—130 (2010)

[4] Leitold, H., Zwattendorfer, B,: STORK: Architecture, Implementation and Pilots. In: ISSE 2010 Securing Electronic Business Processes, 131—142 (2010)

[5] Tauber, A.: Requirements for Electronic Delivery Systems in eGovernment – An Austrian Experience. In: IFIP I3E – Software Services for e-Business and e-Society – IFIP Advances in Information and Communication Technology, 123—133 (2009)

[6] Gennai, F., Martusciello, L., Buzzi, M.: A certified email system for the public administration in Italy. In: IADIS International Conference WWW/Internet, vol. 2, 143—147 (2005)

[7] Dietrich J., Keller-Herder J.: De-Mail – verschlüsselt, authentisch, nachweisbar. In: Datenschutz und Datensicherheit – DuD, vol. 34(5), 299—301 (2010)

[8] Alcalde-Morano, J., Hernández-Ardieta, J., Johnston, A., Martinez, D.,, Zwattendorfer, B., Stern, M.: D5.8.1b Interface Specification, STORK Deliverable (2009)

[9] Witters, J., Overeem, A.: Architecture for delivering pan-European e-Government services (PEGS Infrastructure), version 1.0 (2004)

[10] European Commission: European Interoperability Framework for pan-European e-Government Services, version 1.0 (2004)

[11] Tauber, A., Rössler, T.: Interoperability Challenges for Pan-European Qualified Exchange of Electronic Documents. In: Proceedings of the 9th European Conference on e-Government, 382—390 (2010)

[12] Ferrer-Gomilla, J., Onieva, J., Payeras, M., Lopez, J.: Certified electronic mail: Properties revisited. In: Computers & Security, vol. 29(2), 167—179 (2010)

[13] Tauber, A., Rössler, T. A Scalable Interoperability Architecture for Certified Mail Systems. In: Proceedings of the 12th IEEE International Conference on Commerce and Enterprise Computing, 2010.

[14] Centner, M., Orthacker, C., Bauer, W.: Minimal-Footprint Middleware for the Creation of Qualified Electronic Signatures. In: Proceedings of the 6th International Conference on Web Information Systems and Technologies (2010)

[15] European Commission: The European eGovernment Action Plan 2011-2015, COM(2010) 743, Brussels (2010)

[16] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM), ETSI TS 102 640, v2.1.1 (2010)

[17] Council of Europe: European convention on the service abroad of documents relating to administrative matters. In: European Treaty Series, No. 94 (1977)