STORK 2.0: Breaking New Grounds on eID and Mandates

Herbert Leitold, Secure Information Technology Center, Austria, Herbert.Leitold@a-sit.at
Antonio Lioy, Politecnico di Torino, Dip. di Automatica e Informatica, Italy, lioy@polito.it
Carlos Ribeiro, Instituto Superior Técnico, Portugal, carlos.ribeiro@tecnico.ulisboa.pt

Abstract

The EU Large Scale Pilot "STORK" demonstrated cross-border interoperability of electronic identity (eID) in six production pilots. The lessons learned gave valuable input to a European legal framework on mutual recognition of state's eID schemes. STORK however was limited to interoperability of natural person eID. While such citizen eID interoperability is an important step, many e-government or e-business processes are carried out "on behalf": A natural person acting on behalf of another natural person, a natural person representing a legal person, respectively. Cross-border interoperability of electronic representation and electronic mandates has been a key objective of the STORK follow-up project "STORK 2.0". We discuss how STORK 2.0 has implemented interoperability of electronic representation and how that got applied to its pilots in this paper. We focus on representation of legal persons, as this is essential on removing practical barriers in a digital internal market.

1. Introduction

National electronic identity (eID) initiatives in Europe started in the late 1990's and early 2000's. Meanwhile most EU Member States have issued some form of eID. However, those systems were often developed as national islands; cross-border interoperability has usually not been considered. This is a barrier to the internal market, as citizens and businesses that enjoy the "four freedoms" free movement of people, goods, services and capital in the physical world cannot do so in the online world when it comes to secure authentication.

The EU Large Scale Pilot STORK addressed this by developing solutions for cross-border interoperability of eID systems. STORK has been a success. It ran from 2008 to 2011 and demonstrated technical feasibility of eID federation between 18 EU/EEA Member States. This has been validated in six production pilots as diverse as cross-border authentication at e-government portals, secure chat rooms for minors, or login to European Commission services. From the experience gained it became clear that a main barrier for cross-border eID was lack of a legal basis, which eventually led to policy action – the EU Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) [1]. STORK is assumed to become the technical basis supporting eIDAS.

eID schemes usually first considered authentication of natural persons, so did STORK. While citizens' eID and their cross-border interoperability is a major leap, e-business and e-government processes are in many cases carried out by legal persons or professional representatives. This makes representation and electronic mandates and its cross-border interoperability a logical next step to citizen eID. The importance of representation is also reflected in the eIDAS Regulation, as it includes it in its definition of electronic identification as "*the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person*".

Electronic representation and electronic mandates are addressed by the STORK successor project STORK 2.0. The project started in 2012 and covers 19 EU/EEA Member States. STORK 2.0 builds upon the technical basis of STORK for citizen authentication, but amends by data describing and processes handling electronic mandates. This comes with two main issues: The first issue is that comprehensive mandate systems that seamlessly integrate with national identity management systems (IDM) are still rare. Ad-hoc systems emerged that lead to a high degree of technical heterogeneity. The second issue is that the legal basis of

mandates, its forms and scope significantly differ between states. This gives a challenge to map the mandate to a meaning understood in the receiving state's application.

These aspects are discussed in this paper. We start in section 2 in describing the STORK infrastructure. We sketch pilots and give a view of what areas STORK has been used in. Section 3 continues by giving an overview of mandate systems, in particular on legal person representation. This is the basis of discussing how these systems got integrated in section 4, where using representation in STORK 2.0 pilots is described Finally, conclusions are given.

2. STORK Infrastructure

The STORK project started in May 2008 with an original duration of three years. As a so-called "pilot A" it had been driven by EU and EEA Member States. The project started with 14 states (Austria, Belgium, Estonia, France, Germany, Iceland, Italy, Luxemburg, Portugal, Slovenia, Spain, Sweden, The Netherlands, and United Kingdom), later got extended by further four Member States (Greece, Finland, Lithuania, and Slovak Republic) and to end of 2011. The objective was to define a framework that does not change existing national eID infrastructure, but defines an interoperability layer on top of national systems that supports cross-border eID federation. In a nutshell, the project has been structured in three phases:

- In the first year, common specifications for the framework have been developed.
- In the second year, the common specifications got implemented and deployed.
- The third year was devoted to piloting the framework.

Two interoperability models have been followed: (1) In the first approach, cross-border eID transactions get delegated to a national gateway – a proxy – that hides specifics of national eID tokens and infrastructure from other countries. We refer to this as "proxy model" or "centralized deployment model". (2) In the second approach, the service provider integrates foreign eID tokens using a middleware. We refer to this approach as "middleware model" or "decentralized deployment model". Both models can co-exist and are interoperable.

Figure 1 illustrates the first model – centralized deployment using central national gateways (proxies). A citizen from Member State MS A accesses a service provider (SP) in MS B. The SP delegates authentication to a national gateway that transforms the MS B national protocol to a common STORK protocol. This gateway is referred to as SP-country pan-European proxy service (S-PEPS). The authentication request is routed to a MS A gateway called citizen-country pan-European proxy service (C-PEPS) that finally authenticates the citizen.

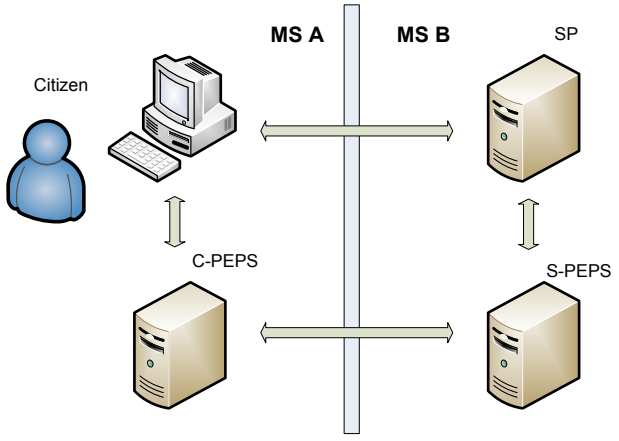

Fig. 1. Centralized STORK deployment model (from [2])

The decentralized deployment model is shown in figure 2. The interoperability component is called a virtual identity provider (V-IDP) that is operated by each SP and integrates the

various eID tokens of those states that follow the model (or routes to a MS-A national gateway “C-PEPS” to bridge the two models. This is, however, not illustrated in figure 2 for sake of simplicity).

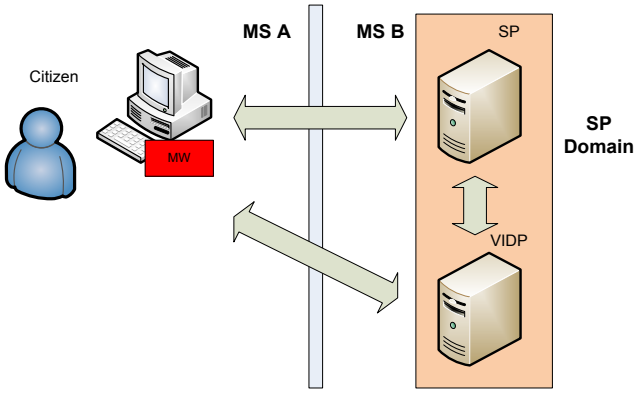

Fig. 2. De-centralized STORK deployment model (from [2])

Whether the centralized or the decentralized approach is followed by a state depends on its existing eID infrastructure, and on liability and data protection considerations. In STORK Austria and Germany have opted for the de-centralized model, all other states have chosen the centralized deployment model.

In fact, both models are interoperable and based on the same federation approach and protocols. Each has pros and cons in terms of scalability, integration, end-to-end security, or liability. The MS choices for models are dependent on weighing those pros and cons and on how the national eID is already integrated. E.g., if a MS already operates a central national authentication gateway, the centralized approach is a logical choice. If a MS however has middleware that get deployed to all SPs, it may continue so and enhance these middleware by foreign eID or PEPS connectors. To bridge between the two models, an S-PEPS also hosts a V-IDP to authenticate middleware country’s citizens, and SP’s V-IDP in the de-centralized model can directly access a C-PEPS. (the two intra-model bridging scenarios are however not shown in figure 1 and figure 2 for sake of simplicity)

A Security Assertion Markup Language version 2 (SAML 2.0) [3] profile has been defined as the common cross-border protocol. It uses a Web single sign-on (WebSSO) profile and a HTTP POST binding. The details of the conceptual models, their differences, and their implementation are described in [2], the detailed specifications are publicly available [4], as well as open source reference implementation of both PEPS and V-IDP.

SAML authentication federation is no novelty. The key objective of STORK was to demonstrate its applicability cross-borders and to gain experience in six production pilots:

1. The first pilot *Cross-Border Authentication Platform for Electronic Services* aimed at integrating the STORK framework to eGovernment portals, thus allowing citizens to authenticate using their electronic eID. The portals can range from sector-specific portals such as the Belgian “Limosa” application for migrant workers to regional portals serving various sectors such as the Baden-Württemberg “service-bw” portal or national portals as the Austrian “myhelp.gv” for personalized e-government services.
2. In the *Safer Chat* pilot juveniles shall communicate between themselves safely. The pilot was carried out between several schools. The specific requirement is that in the authentication process the age group delivered by the eID is evaluated to grant access. Unique identification that is the basis of the other pilots is less important.
3. *Student Mobility* supports exchange of university students, e.g. under the Erasmus exchange program. As many universities nowadays have electronic campus management systems giving services to their students, STORK allowed foreign

students to enroll from abroad using their eID and to access the campus management system's services during their stay, respectively. The prime requirement is authentication, as in the first pilot on cross-border authentication.

4. The fourth pilot *Electronic Delivery* objective is cross-border qualified registered delivery, replacing registered letters by electronic means. On the one hand, delivering cross-border requires protocol conversions between the national electronic delivery standards. On the other hand, registered delivery usually asks for signed proof of receipts. The latter – proof of receipts – is the specific requirement in this pilot. This enabled cross-border use of signature-functions that most national eIDs have.
5. To facilitate moving house across borders, the *Change of Address* has been piloted. In addition to authentication, the pilot focuses on transfer of attributes, i.e. the address.
6. The European Commission Authentication Service (ECAS) is an authentication platform that serves an ecosystem of applications that are operated by the European Commission. Member States use these services to communicate among themselves and with the EU institutions. Piloting administration-to-administration (A2A) services with national eIDs was a STORK objective. The pilot *A2A Services and ECAS Integration* serves this objective by linking up STORK to ECAS.

A major outcome of STORK was the classification of national eID systems into assurance classes – so-called Quality Authentication Assurance (QAA) to establish trust. Four QAA ratings – minimum, low, substantial, and high – are defined. The classification is comparable to Levels of Assurance (LoA) defined as trust ratings for US administration. The process is that the services providers request a certain minimum QAA level in the authentication request. This request gets delivered to the actual authentication process of the citizen, the components (PEPS or V-IDP) ensure that just eIDs meeting the requested QAA level (or above) get accepted to participate in the authentication process.

3. Electronic Mandates and Representation

At first sight, one might consider electronic representation a not too complex task. Work has been done on delegation in role-based access control (RBAC) by [5], or with a permission-based delegation model in RBAC by [6]. Such systems however rather link delegation to intra-organisation identity management (IDM), whereas mandating in national IDM asks for open systems serving a heterogeneous landscape of public administration or private sector systems. An alternative approach seen in literature is linking the mandate to a PKI by using attribute certificates [7]. Attribute certificates can e.g. assert the function of a person holding a X.509 certificate. Legal representation is however not limited to the role of a person, think e.g. of mandating an agent for one single action, such as licensing a car.

Representations have been categorized by [8] into (1) bilateral representations (also referred to as "direct mandates" between a mandator and a proxy), (2) substitution (an indirect representation where the mandator empowers an intermediary that delegates to the proxy), and (3) delegation (a direct representation initiated by an intermediary).

In the various scenarios, empowerment can be based on a:

a) Constitutive Register (Commercial Register, Register of Associations, …),
b) Competent Authority (asserting a profession, e.g. tax accountant or lawyer), or
c) Willful Act (mandate established by a person).

In this paper we focus on legal person representation. This for sake of simplicity and as it already covers the three cases above: The legal representative(s) (e.g. CEO, Board) often get registered to a Constitutive Register, e.g. the Commercial Register as in case a) above. In many legislations, professional representatives like tax accountants do not need an explicit mandate, the sole fact that a legal person is a client together with an assertion that the representative is a professional representative suffices to act on behalf of other persons. This assertion is then by a Competent Authority (e.g. the Bar Council) and not directly bound to a

particular Constitutive Register the legal person is enrolled to, which leads to case b) above. The third case c) occurs when legal representatives give a bilateral mandate to staff members or subcontractors, like to carry out a certain purchase. If proving that a certain representation is valid is needed to perform a certain action, both the mandate by the legal representative (e.g. CEO) to staff member/subcontractor, and the fact that the mandator is the legal representative (the CEO) of the principal (the legal person) need to be verified. This is referred to as chained mandates.

A national mandate system that covers all three cases and its combinations can be called systematic mandate management. A study contracted by the European Commission that has been carried out in 2009 revealed, that systematic mandate management is rare in European states [9]: "*[…] a systematic approach to mandate management and authorisation functionality – i.e. the ability to allocate, retract or verify specific permissions of a specific entity - in the examined eIDM systems was still altogether rare. 22 countries out of 32 (69%) have no form of mandate/authorisation management, other than the allocation of certificates or credentials to the representatives of a specific legal entity. 8 countries out of 32 (25%) have implemented an ad hoc form of mandate/authorisation management covering specific applications or service types; and only two countries have implemented systems of mandate/authorisation management which can be characterised as systematic: in Austria, an open approach to mandates based on signed XML records was adopted, and Belgium is currently implementing a systematic approach to manage authorisations.*"

The study mentioned above was published in 2009. Meanwhile several other Member States launched systematic approaches. Still a heterogeneous landscape is given and a challenge STORK 2.0 had to overcome was to federate between those systems. While this is somehow similar to federation between heterogeneous eID, the situation with mandates adds a degree of complexity: The concept on natural person identity and how to uniquely represent it is pretty similar across states (still differences exist e.g. in the use of identifiers). How representation is established and what is the actual right associated with it, differs significantly. In particular the actual powers that are assigned by national law to certain "pre-defined" representation like "procura", that exists in some Member States, differ. Those differences exist also in traditional paper-based processes, but as soon as relying parties open online processes that make automatic decisions and that rely on national definitions of representation powers, differences matter.

To get a topical view on mandates and representation, STORK 2.0 surveyed its participating states. The conclusion of this survey on legal person representation was (from [10]): Most Member States require that companies be registered in a Commercial Register, although the exact name and nature of the service varies in each Member State. Upon registration each company is given a number that identifies the company. Some of these numbers are simple sequential numbers others are smart-numbers that not only identify the company but also the branch of the company, but they always identify the company. By opposition to citizens, companies do not act by themselves, they are represented by citizens. However, most Member States have authentication tokens specific for companies. Most of these tokens are hardware tokens containing qualified certificates that can be used not only for authentication but also for signing documents in the name of the company. It should be noticed that, although these tokens are used exclusively to represent companies, they are nominative, i.e. they contain the identity of the representatives. Most of these tokens are however sector-specific (financial, administrative, legal, banking, health, etc.). Different sectors do not share their tokens, even if they refer to the same company and representative.

In addition to such specific legal person tokens, the survey [10] describes mandate systems that some Member States introduced by linking Constitutive Registers and specific Mandate Registers with the citizen eID systems. Examples are the Mandate Issuing Service [11] in Austria, the X-Roads interconnection of Portals and Registers in Estonia, or the eRecognition system in the Netherlands.

4. Representation in STORK 2.0

To introduce representation and mandates to STORK 2.0, the same phases as in the predecessor project got applied:

- A stock taking phase in which each Member State involved described its traditional system of representation and mandates, including electronic mandate systems. Special attention was given to credentials required to access online pilot services.
- The specification phase extended the existing STORK process flows adding new actors and information concerning legal persons and the powers to represent them. Specifications were implemented and integrated into the pilot production systems.
- The piloting year includes continuous monitoring of SMART success criteria (Specific, Measurable, Achievable, Relevant, and Time-bound) and is accompanied by three formal evaluations to ensure adequate assessment of activity and achievements.

STORK 2.0 builds on the STORK infrastructure. It extends with the secure exchange of information verifying the existence of companies in national business registers, or in equivalent public authorities, and validating the powers of the authenticated person to act on behalf of the company. Two additional process flows have been introduced [11]:

- *Authentication on Behalf* extends the standard authentication request of the natural person by attributes describing the representation powers. These are queried by attribute provider (AttP) like Company Registers or specific Mandate Registers. Alternatively, the powers may be stored in the authentication credential itself, like an attribute certificate that exists in some Member States. The actual source of the assertion is Member State specific, and can even coexist within the same state (i.e. a state may have several sources of attributes). What STORK 2.0 does is to map all these attributes with different sources and formats to a common protocol and a common quality scheme for attributes (using the synergy with eID quality scheme "QAA" that has been introduced in STORK, we refer to attribute quality as "AQAA"). In a nutshell, the Authentication on Behalf request gets the representative authenticated and delivers the authentication result and associated representation powers in a single response to the service provider.
- The *Powers* request is similar to authentication on behalf, but the assertion by an authoritative source is delivered out of band, like a scanned excerpt of a Company Register or a notary deed. The representative states the representation and the represented person in the authentication process and self-asserts the powers using a digital signature.

The first case "Authentication on Behalf" is applied where advanced infrastructure exists that allows to derive a representation assertion online. It allows for automated processing at the relying party, as long as the representation powers are machine-processible, like not containing constraints in free text. The second case is useful when such infrastructure does not yet exist in the source state, but still semi-automatic processing can be applied, like manually checking if the out-of band assertion by an authoritative source matches the ad-hoc representation claimed by signing a self-declaration.

The challenge lies less in integrating mandate data into the existing process flows and protocols, but in overcoming national differences, like those described in the previous section. Two aspects are important: Trust and semantic differences.

On the first aspect – trust – a service provider needs the information of whether the representation powers are highly reliable like e.g. settled by an authoritative source, or whether they are less certain like e.g. been self-declared by the representative. The QAA model that was defined for security levels of the eID credential got extended to an Attribute Quality Authentication Assurance (AQAA). Attributes are assigned an AQAA value defining four quality levels, as for QAA distinguishing minimal, low, substantial, or high assurance.

On the second aspect – semantics differences – STORK 2.0 defined a mandate taxonomy. It allows mapping of national specifics to a common mandate representation. It defines types of powers like general powers, commercial powers, or human resources powers. With this

definition, the STORK 2.0 components enter into a semantic transformation that goes beyond of what existed in STORK: STORK did some technical transformations like mapping national identifiers to a common data set. This however has little effect on the actual meaning of the identifier. By mapping a legal fact like the representation powers of an agent, a semantic transformation is given that has legal consequences. For instance, the notion of a "procura" that exists in just some states assigns general powers, but is limited to day-to-day management duties. By mapping a procura to general powers, a service receiving it and interpreting a general power under a local notion of full powers might be mislead.

STORK 2.0 defines four production pilots to gain experience needed to proceed to a workable cross-border electronic mandate system. These pilots – including its relation to legal person identification, which is the main scope of this paper – are:

1. eAcademia aims at facilitating the exchange of academic attributes like certificates acquired in course. The pilot is mainly concerned with attributes and attribute providers that goes beyond the scope of this paper. Legal person authentication is less relevant, although it is required in the Job Selection service where companies, or their legal representatives, submit cross-border job offers that are then applied for by students or former students.
2. eBanking shall allow opening bank accounts cross-borders and to access these accounts online. The first phase of the pilot is bank accounts for natural persons, mainly related to the fact that banking laws already gives significant challenges on opening bank accounts cross-borders as natural persons acting on their own behalf. With representation in later stages it allows managing a company's bank account.
3. eHealth will support the Patients Rights Directive allowing cross-border access to health records. Representation allows mandating family members or health care professionals. Legal person representation is just addressed if the health care professional is an organisation, like a hospital.
4. The Public Services for Business pilot shall enable businesses to make use of e-government services in other countries. This is the pilot where the core benefit of legal person identification gets seen. The pilot allows for registering a business or accessing a business service portal cross-borders the same way a local company does.

5. Conclusions

The paper discussed how the STORK 2.0 Large Scale Pilot addresses cross-border interoperability of representation and mandates to authenticate to an online service on behalf of other persons. It bases on the results of the predecessor project STORK that established such an interoperability framework for natural person authentication. This framework got extended by binding the natural person authentication to the principal she represents. This is done by additional attributes that assert such representation. The assertions get derived from third sources like Constitutive Registers or Competent Authorities. The overall concept introduced by STORK has been kept, i.e. to de-couple national systems by federating between them. National specifics got mapped to a common protocol and the SAML 2.0 STORK profile got extended.

The lesson learned is that such mapping gets more complex for representation and mandates as attributes of the acting person, as it was the case when natural persons did act on their own behalf. The reason is that the concept of natural person authentication is pretty similar in all states, so are simple attributes associated with the natural person like name, date of birth, or an address – neglecting national syntactic or semantic differences for such attributes, that easily can get mapped semantically. With mandates and representations, however, an additional layer of complexity is introduced, as a mandate describes a certain right the representative has. Such rights can be pretty specific and bound to a national situation. Thus, semantic mapping is not at all easy. STORK 2.0 managed this by introducing

a mandate taxonomy that defines a limited set of mandates and roles. These get mapped at the source and destination STORK infrastructure components.

We limited the scope of the paper to legal person representation. This case gets mainly tested in a pilot on Public Service for Businesses, where company registration and access to national business service portals is enabled. Legal person representation has some role in the other pilots – in eBanking to open a bank account on behalf of an organization, eHealth where a health care provider accessing a patient's health record can be a hospital represented by the doctor that gives care, and eAcademia to allow businesses to interact with students and former students.

Aside legal person representation, STORK 2.0 also pilots representing natural persons. Examples are professional representation like a lawyer representing a client, or a family member or health care provider representing a patient. The underlying concepts are however the same, thus STORK 2.0 is applicable to a wide range of cases.

At time of writing this paper the pilots have just started. It therefore would be inappropriate to already claim lessons learned from actual real-world piloting. The work on in-depth surveying the Member State systems and the experience gained in mapping those to a common protocol is already considered a significant result. It is expected that these STORK 2.0 results give valuable input to the ongoing work on implementing acts related to the eIDAS Regulation on legal person identification, as the predecessor project STORK already did for natural person identification.

6. References

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[2] Leitold, Herbert; Zwattendorfer, Bernd: STORK: Architecture, Implementation and Pilots. In: ISSE 2010 Securing Electronic Business Processes, Vieweg+Teubner, pp. 131-142

[3] Cantor, Scott; Kemp, John; Philpott, Rob; Maler, Eve: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 2005.

[4] Alcalde-Morano, Joaquín; López Hernández-Ardieta, Jorge; Johnston, Adrian; Martinez, Daniel; Zwattendorfer, Bernd; Stern, Marc; Heppe, John: Interface Specification, STORK Deliverable D5.8.3b, 2012.

[5] Khambhammettu, Hemanth; Crampton, Jason: Delegation in Role-Based Access Control, In: Proceedings of ESORICS'2006. pp.174-191

[6] Zhang, Xinwen; Oh, Sejong; Sandhu, Ravi: PBDM: A Flexible Delegation Model in RBAC. In: Proceedings of the eighth ACM symposium on Access control models and technologies SACMAT 2003, pp. 149-157

[7] Farrell, Stephen; Housley, Russ; Turner, Sean: An Internet Attribute Certificate Profile for Authorization. IETF RFC 5755, 2010

[8] Rössler, Thomas: Empowerment through Electronic Mandate – Best Practice Austria. In: Proceedings of 9th IFIP WG 6.1 Conference on e-Business, e-Services and e-Society, I3E 2009, Editor: Springer, IFIP Advances in Information and Communication Technology, 2009, Volume 305/2009, pp. 148-160

[9] European Commission: Study on eID Interoperability for PEGS: Update of Country Profiles. IDABC Programme, 2009

[10] STORK 2.0: Existing e-ID infrastructure analysis, STORK 2.0 deliverable D2.1, 2013

[11] Tauber, Arne; Leitold, Herbert: STORK: Architecture, Implementation and Pilots. In: ISSE 2011 Securing Electronic Business Processes, Vieweg+Teubner, pp. 224-234

[12] Heppe, John (lead editor) et al.: First version of Technical Specifications for the cross border Interface, STORK 2.0 Deliverable D4.4, 2013.