STORK 2.0 – Summary of WP3 outputs (M1-M14)

Introduction

This note is intended to provide a summary of the current status of the STORK 2.0 WP3 efforts. It acts as an executive summary across the various deliverables of WP3, allowing the reader to quickly get acquainted with the main outputs without reading the full deliverables, and to present the main questions to be addressed within STORK 2.0.

In the sections below, each deliverable is given a one page summary to outline its scope, followed by a green box outlining the main findings.

For more details, we refer to the full deliverables.

Legal analysis – D3.1

Scope of the deliverable and main results

STORK 2.0 (like STORK1) operates without any specific formal trust model/governance framework (other than the consortium agreement, contract with the Commission, and the legal framework of the eSignatures Directive and its national transpositions. This deliverable examines whether this is sufficient, and what further steps might be needed. It makes a distinction between the shorter term (i.e. the operation of STORK 2.0 during the project, when no new legislation can be anticipated) and the longer term (i.e. the sustainability of STORK 2.0 outputs after the project, building on the assumption that the proposed eID and Trust Services Regulation or a substantially similar text is adopted).

Main outputs

- The deliverable firstly analysis the general structure and operation of STORK, including an identification of the various categories of stakeholders (End User, Service Provider, PEPS operator, V-IDP operator, Identity Provider, Attribute Provider, and the potential future Attribute Aggregator; the role of governance/maintenance of STORK components by a Governing Entity is examined in less detail). The main legal risks are analysed for each category, including notably applicable rules, dispute resolution, data protection, liability, service level assurances, mandate representation, and case-specific challenges (health data, financial services rules, and transfers of personal data outside the EU/EEA).
- These legal challenges are then mapped against the existing legal framework (mainly the eSignatures Directive and the proposed eID and Trust Services Regulation), and against the choices made in other LSPs. On the latter point, mainly epSOS and PEPPOL are instructive, since they provided specific agreements that could be concluded between the participants in the relevant trusted networks.
- The deliverable proposes that STORK2.0 follows the same approach, using standardised contracts as a way of clarifying the roles, responsibilities and liabilities of (in particular) the PEPS/V-IDP Operators, which is the main legal issue falling within the scope of STORK to be resolved today. The PEPS/V-IDP Operators form a trusted network that can also be used to impact how relationships with other stakeholders (such as the IDPs and the APs) can be governed: if the PEPS/V-IDP Operators know they obligations and liabilities, they can conclude back-to-back agreements with IDPs and APs (if they feel this is beneficial) to ensure all participants in the network know their duties and risks. Some legal challenges faced by the stakeholders are not impacted by this proposed approach (e.g. how do Service Providers comply with data protection laws?), but these are issues external to STORK that we do not need to solve.
- This proposal does not impact pure MW countries, because they rely solely on the existing legal framework for eSignatures.

- It should be noted that this contractual approach is primarily needed as a temporary solution until the entry into force of the eID and Trust Services Regulation (assuming that this will happen at some point), but it is not impossible that such an agreement would be necessary or beneficial even after the entry into force, given the need to also address issues that are not addressed in the (current draft of the) Regulation, such as the role and responsibilities of Attribute Providers, and the measures to be taken by the PEPS/V-IDP Operators to ensure their compliance with applicable rules within the network.
- On the basis of this analysis, it is proposed that a contractual framework is drafted to govern the relationship between PEPS/V-IDPs, building on the examples of epSOS and PEPPOL.

Quality authentication assurance – D3.2

Scope of the deliverable and main results

One of the primary outputs of STORK 1 was the QAA (Quality Authentication Assurance) model, which permitted quality levels to be assigned to various eID solutions, based on some of their main characteristics. This deliverable updates that model to cover external attribute providers as well, and provides sustainability recommendations for the existing QAA policy (particularly by comparing it to ongoing international standardisation work.

Main outputs

- A new Attribute Quality Authentication Assurance (AQAA) framework is proposed, covering external attribute providers. Criteria are based strongly on the existing QAA with small changes to account for the unique characteristics of APs compared to IDPs. The criteria include validation of the link between the eID and the attribute (both at the time of registration and when authenticating), the validation of the quality of the attribute, and the quality of the attribute provider itself.
- The main challenge is the linking between eID and attribute information at the time of authentication. The following possibilities are distinguished in the deliverable:
    - The AP uses the STORK eID to retrieve attribute information (either because the user uses his eID to authenticate towards the AP, or because it uses a SAML assertion from a PEPS/V-IDP to retrieve attribute information):
        - If the AP uses the STORK identifier, it can retrieve attributes with perfect reliability. However, this is not expected to happen in practice.
        - If the AP does not use the STORK identifier, fuzzy logic could be used (based on matching name, date of birth, nationality, etc), but the quality of the attribute assertion would suffer significantly. Criteria to asses this negative impact are proposed in the AQAA.
    - The AP doesn't use any STORK eID, but requires re-authentication using its own (non-STORK supported) credentials. In this case, STORK cannot provide any statement on the quality of the attribute assertion, because the quality of the AP's credentials are unknown. While a statement could again be made on the likelihood of matches (based again on fuzzy matching between the AP's information and STORK's information), this would only be on an FYI basis without assurances.
- The role of attribute aggregators and their impact on the AQAA is briefly discussed, but not elaborated in detail because it is not yet known if/how this would be implemented.
- With respect to sustainability, the existing QAA is compared to the emerging ISO/IEC FDIS 29115 standard, which could conceivably replace STORK's QAA. The deliverable recommends however to retain the QAA, because the ISO standard is unfinished and is not adjusted to the specific characteristics of many EU eID systems. At any rate, maintenance of the QAA is the responsibility of the ISA Programme, and will thus not need to be addressed by STORK.

Legal entities identification and mandate management – D3.3 and D3.5

Scope of the deliverables and main results

STORK 2.0 implies the integration of legal entities and mandates (both mandates to represent legal entities and contractual mandates to represent specific natural persons). While these are separate topics covered by separate deliverables, they are relatively similar and the deliverables have been strongly aligned. For this reason, they are also discussed jointly in the present document.

Main outputs

- Both deliverables analyse the legal rules in each country, on the basis of the aforementioned questionnaires. Topics included key concepts, establishment of mandates (form, content and notary intervention), validation obligations by the recipient of a mandate, legal limitations, term and revocation, use of submandates, and of course the establishment of mandates using electronic means (including the need for eSignatures).
- As expected, both deliverables note that the national frameworks are largely unaligned, and often contain specific exceptions (linked to the type of legal entity, the type of transaction conducted, corporate statutes, etc).
- For D3.5 (legal entities), the main challenge will be the integration of business registers as attribute providers in such a way that natural persons identified through STORK can be reliably linked to a legal entity. The second stage (establishing whether they are competent to represent that legal entity for the specific envisaged transaction can be done by:
    - Creating an ontology of mandates that are most commonly used. While this will not be comprehensive or cover all national rules, variants and exceptions, it should provide a workable simplification of legal reality. This ontology has been drafted in cooperation between WP2-3-4.
    - Requiring a matching of this ontology against the know relationship that the identified person has with a legal entity (i.e. 'does person x with function y in company z have the mandate in this ontology'), and requiring a confirmation on this point.

  While not entirely comprehensive, this approach should be functional and sufficient in most cases, and at least far superior to the assurances provided in paper transactions.
- For D3.3 (mandates in general), the analysis pointed out that this topic is similarly governed by national law, and that it would be necessary to assess in each case which law applied, which type of mandate was being given under national law, and what the relevant requirements would be. As a pragmatic way forward, it may be advisable to construct mandate modelling solutions on the basis of the examples provided in e.g. Austria, and to assess on a case-by-case basis whether this approach is suitable for a given use case. Again, the use of affirmative declarations by mandate givers/mandate holders can be useful as a risk mitigation approach.

Data protection – D3.7

Scope of the deliverable and main results

The deliverable aims to identify and address data protection (privacy) compliance challenges in STORK 2.0. Within STORK1, this topic was addressed through contacts with the Article 29 Working Party, which consists of representatives of the national Data Protection Authorities as well as the European Data Protection Supervisor, thus acting as an authority on ensuring data protection compliance.

These contacts brought up a series of questions, including on the allocation of the roles of data controllers versus data processors (i.e. who is responsible for data processing in STORK) in the PEPS and MW models, and questioning why both existed. New challenges in STORK 2.0 include particularly the role of external attribute providers, the processing of sensitive personal data (notably health data), and the transfer of personal data to service providers in countries where EU data protection rules do not apply (notably in Turkey[1]).

Main outputs

- A comparative privacy risk analysis (a privacy impact assessment) was drafted between the PEPS/MW models, explaining their strengths and weaknesses and arguing that neither was clearly superior, so that both should be retained.
- A proposal was made on the allocation of roles (controller/processor) for the PEPS and MW models, in which:
    - In a MW-MW model, the service provider clearly acts as a data controller, and no data processor is necessarily present.
    - In a PEPS-PEPS model:
        - The PEPS operator acts as a data processor to the SP for the authentication processes conducted on behalf of the SP, with the SP acting as the data controller.
        - The PEPS operator acts as a data controller for any other processing of personal data, notably any logging of authentication processes that may be done by the PEPS.
    - Mixed models (MW-PEPS) will similarly involve PEPS/V-IDP operators to act as data processors to the SP for authentication processes, and as data controllers for any other (own purposes).
    - This model would imply the need for data processing agreements in PEPS/V-IDP based models, which can however be standardised through generic terms and conditions.

[1] The EU Data Protection Directive applies in the EU Member States and EEA Countries (thus including Iceland). Furthermore, Swiss data protection law has been found by the EU Commission to be equivalent to the Directive. Therefore, there are only specific transfer compliance questions for Turkey, which is not an EU/EEA country and has not been confirmed to have equivalent laws.

    - It should be stressed that the proposal above was not presented as a definitive conclusion within STORK nor as the *only* viable interpretation, but rather as the basis for discussions with the Article 29 WP.

- The integration of external attribute providers can be implemented in various ways. The most logical perspective is that (for the purposes of integration within STORK2.0) the APs would be integrated as (sub)processors to the PEPS/V-IDPs. STORK2.0 could propose standard terms that the PEPS/V-IDP operators could use to implement this.
- For the processing of sensitive personal data, the processing of health data within STORK2.0 would present specific compliance challenges, which may vary from country to country. However, if health data is processed only through infrastructure external to STORK2.0 (namely the epSOS infrastructure), then this problem will not present itself.
- Finally, the transfer of personal data to service providers outside of the EU (in practice Turkey) is problematic. If the SPs indeed act as data controllers (as proposed above), EU data protection laws currently imply that Turkish SPs would need to comply with all national data protection laws (i.e. all laws of all MS/EEA countries that participate in STORK2.0). This would be extremely burdensome, and may not be viable in practice. Therefore, it was suggested to integrate Turkish service providers on the basis of the rules of the newly proposed Data Protection Regulation (which would act as a single applicable law). While not strictly legally compliant, this would have the benefit of feasibility and of being future-oriented.
- All of the points above were circulated within STORK2.0, and thereafter submitted in the form of a summary note to the Article 20 Working Party, for discussion purposes only. No feedback was received so far.