Written report of the

Article 29 Data Protection Working Party

Biometrics & eGovernment Subgroup

SECURE
IDENTITY
ACROSS
BORDERS
LINKED

Description:

Overview:

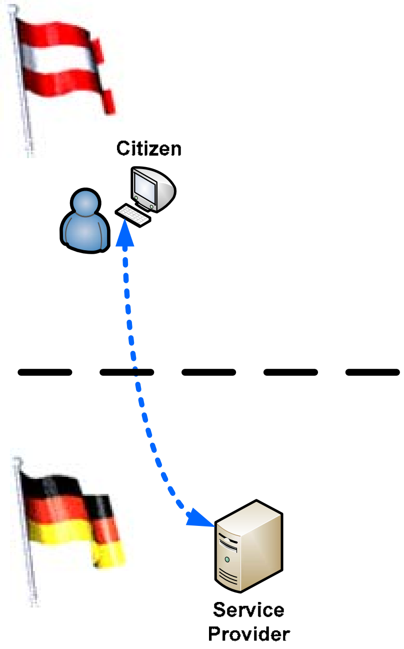
STORK is a large scale pilot under the ICT-PSP (Information and Communication Technology Policy Support Programme) of the competitiveness and innovation framework programme, co-funded by the EU. It aims at implementing an EU wide interoperable system for recognition of electronic identities (eID) and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State. It piloted transborder eGovernment identity services and learned from practice on how to roll out such services, and to experience what benefits and challenges an EU wide interoperability system for recognition of eID will bring.

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

2 basic models have been developed:

For the interconnection of member States eIDs infrastructures, STORK has developed and piloted one Interoperability Framework, based on 2 basic models:

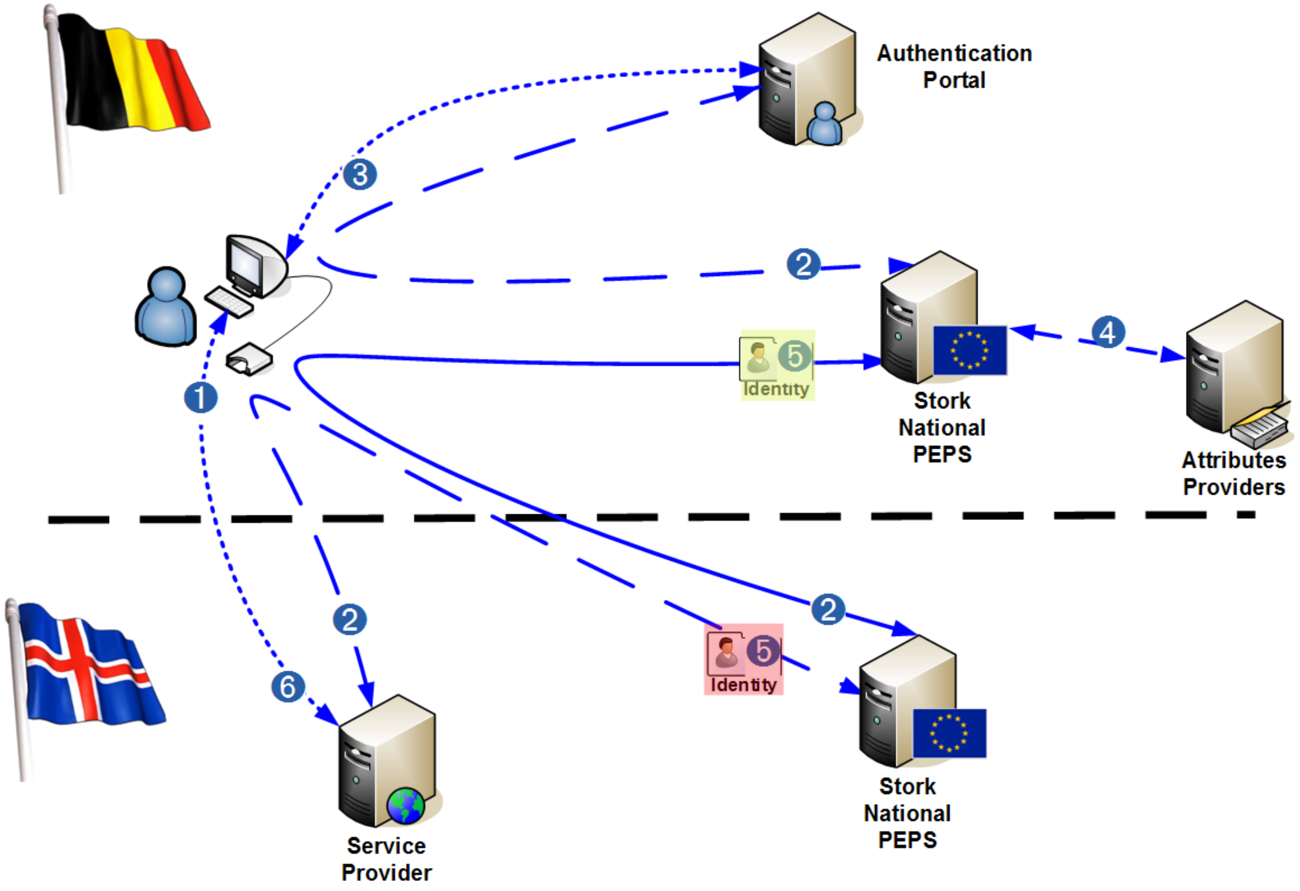
Middleware model (MW)



In the middleware model the Service Provider uses software components (a middleware "SPware") that implement a direct communication with the foreign eID token.

The citizen communicates directly with the foreign Service Provider and no intermediaries are in between.

Pan-European Proxy Services model (PEPS)

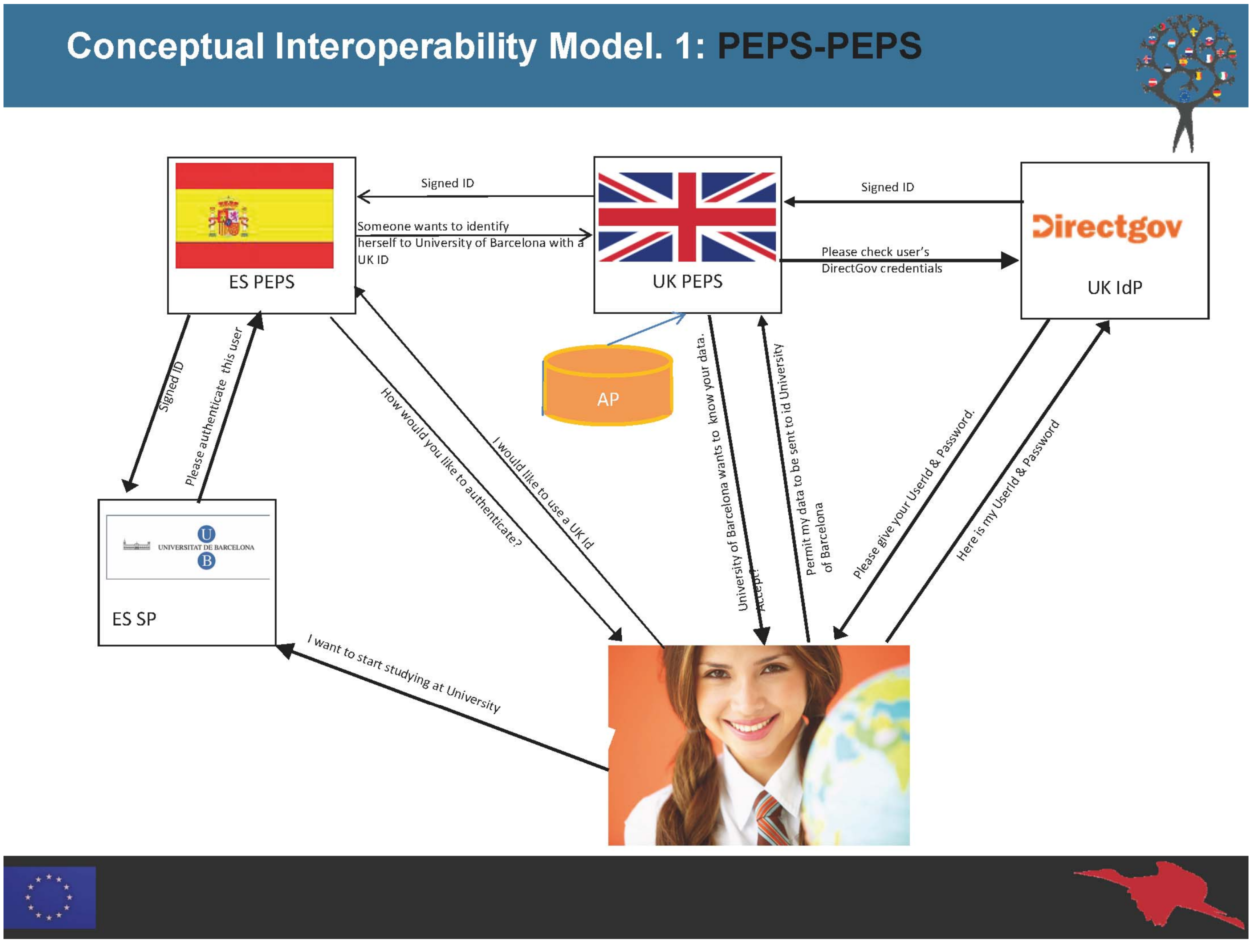


Identity data exchange between MS takes place through the Proxies or PEPS.

The PEPS acts a single gateway of this Member State’s eIDs towards other countries and it acts as an intermediary for foreign eIDs towards its domestic Service Providers.

The electronic authentication process takes place at the country where the eID is being issued.

The concept foresees PEPS in each country that chooses this model. To put only one single PEPS in the EU in operation is not foreseen.



Conceptual Interoperability Model. 1: PEPS-PEPS

ES PEPS

Signed ID

Someone wants to identify herself to University of Barcelona with a UK ID

UK PEPS

Signed ID

Please check user's DirectGov credentials

Directgov

UK IdP

AP

Signed ID

Please authenticate this user

UNIVERSITAT DE BARCELONA

ES SP

How would you like to authenticate?

I would like to use a UK Id

University of Barcelona wants to know your data. Accept?

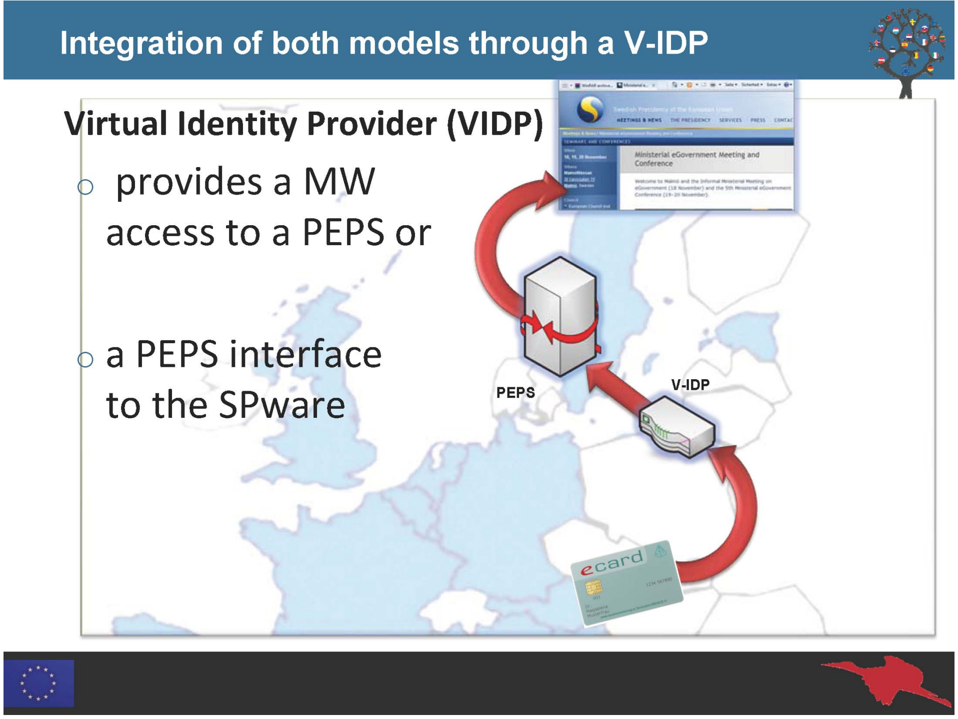
Permit my data to be sent to id University of Barcelona

Please give your UserId & Password.

Here is my UserId & Password

I want to start studying at University

... and how to combine them (MW-MW, PEPS-PEPS, MW-PEPS, PEPS-MW)



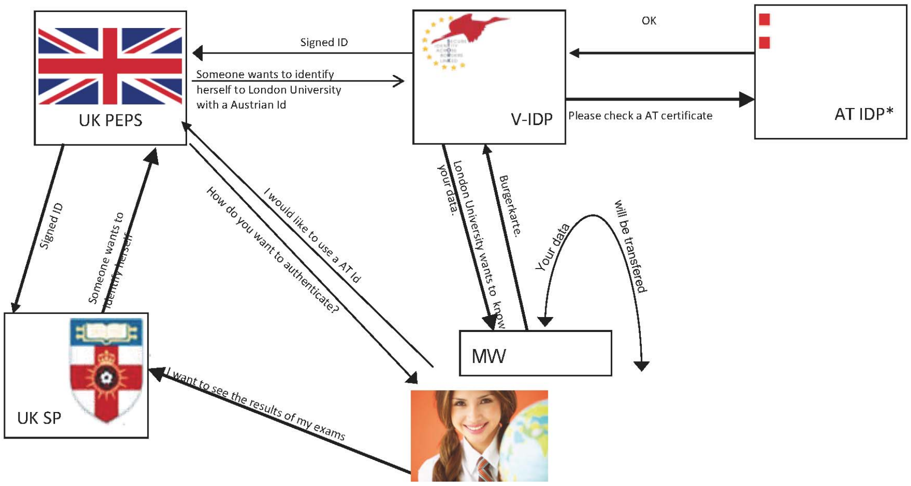
Integration of both models through a V-IDP

Virtual Identity Provider (VIDP)

- provides a MW access to a PEPS or
- a PEPS interface to the SPware

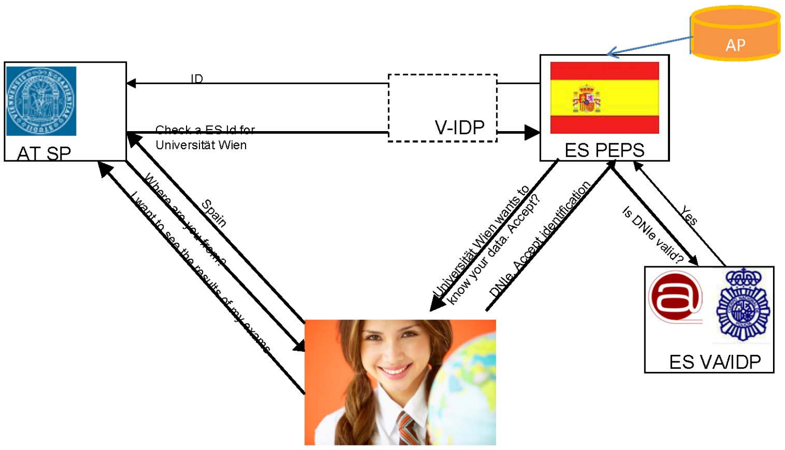
Integration of the PEPS-MW model

If the citizen from a “middleware country” accesses a Service Provider in a “PEPS country”, the Service Provider redirects to the foreign PEPS as if it was a PEPS-to-PEPS case


UK PEPS
Signed ID
Someone wants to identify herself to London University with a Austrian Id
V-IDP
OK
Please check a AT certificate
AT IDP*
Signed ID
Someone wants to identify herself
I would like to use a AT Id
How do you want to authenticate?
London University wants to know your data.
Burgerkarte.
Your data
will be transfered
MW
UK SP
I want to see the results of my exams

Conceptual Interoperability Model. 4: MW-PEPS

- The Service Provider redirects directly to the foreign PEPS (in the service provider state) which carries out and asserts the authentication.


AP
AT SP
ID
Check a ES Id for Universität Wien
V-IDP
ES PEPS
Where are you from?
Spain
I want to see the results of my exams
Universität Wien wants to know your data. Accept?
DNIe. Accept identification
Is DNIe valid?
Yes
ES VA/IDP

The common specifications have been designed so that major components operate on the same protocols, irrespective of the model or its combinations.

The software used on the PEPS and the MW software running at the service providers environment are updated and developed synchronously. The main difference between the 2 model is that in the PEPS scenario the service provider outsources the handling of the electronic identification and authentification process to a PEPS provider while in the MW scenario all is done by the controller himself.

Specific questions:

Data controller / data processor:

The subgroup sought for clarification on who is data controller and who is data processor in the course of processing and transferring personal data within the STORK project. Which bodies do collect, process and store which data? Are there transfers of personal data to third parties? This clarification is also important to establish the responsibility of the different bodies involved in the Stork system and to determine the respective data protection supervisory authority.

Conclusion:

In the middleware model the answer to that question is clear. Because all processing including the processing of the STORK specific operations is done by the controller that receives the citizens request (the service provider “SP” in the figures above) there are no data transfers to third parties. The service provider (SP) is therefore responsible as controller for all personal data used during the identification and authentification procedures developed and provided by STORK.

In the PEPS model it can be argued that the PEPS (pan European proxy service) is a data controller as far as the electronic identity management is concerned. He processes personal data, transfers them to another PEPS and also handles the replies (signed IDs or rejection). Although the PEPS is a service provided to different institutions (service providers “SP” in the figures above), these are not in control of what happens in the PEPS. The only thing a SP provider is in control of is to either accept or refuse the offer of a PEPS provider.

It can also be argued that the service provider (SP) as controller of the service provided to the citizen chooses to use the services of a PEPS and therefore the

PEPS is only a processor acting on behalf of the service provider (SP). This interpretation has one practical disadvantage from the point of view of the aim of reducing administrative burdens. If a PEPS is considered as processor this creates a significant number of controllers of this PEPS (all that use this PEPS). As a consequence all this controllers will have to notify the PEPS as one of their data processings.

This is a typical dilemma that comes with the phenomena of “electronic portals”. The WP29 did not come to a conclusion in WP 169. Example 11 describes the problem, however leaves it open whether a portal has to be considered as a controller or not. In line with WP 169 the subgroup wasn’t able to come to a concordant conclusion. Some of the subgroup members would consider the PEPS as controller and some as processor.

Therefore controllers that use a PEPS and provider of PEPS services will have to decide if they consider themselves as controller or processor under the Directive 95/46 and contact their national DPA to confirm this for example during a notification procedure.

Data security:

The subgroup considered that data security measures are of high importance especially because of the transnational character of the application and enquired which measures are foreseen (e.g. end-to-end encryption) and what is foreseen to prevent hijacking of STORK partner or services websites.

The STORK project partners stated that common minimum requirements have been established. End-to-end security has been implemented. The technical standard of the interoperability tools is in many cases higher then the local standards used to access eGovernment services. Segmented technical encryption (SSL, SAML re-signing) is implemented.

However all communication is routed through the users browser and therefore the risk of a man in the middle attack has to be taken into consideration for both models, especially in the PEPS model because of the post-redirection via the users browser. STORK should further make sure to counter the typical risks of the centralised architecture of the PEPS model where much more transactions are processed for each request. STORK should implement a continuous surveillance of the system to make sure to be able to discover and counter risks that occur during the transactions.

Further a comparative risk analysis of both models should be carried out. It appears that a lot of effort is required to make those 2 models interoperable. A privacy impact assessment has not been made on which basis the WP 29 could judge if one of the both models poses a higher privacy risk than the other. A recommendation to use only one of the 2 models in order to conform to the principle of necessity and the choice of the least intrusive option can therefore not be made yet.

Beyond the core infrastructure that has been built by the STORK project partners, no common standards are specified. STORK relies here on national responsibility. There are indeed common EU standards that have to be met eg. the requirements set up for eSignatures. STORK seems to wait for Digital Agenda Key Action 16 (eID – electronic identities) and Key Action 3 ("eSignature Directive") to cover/clarify the open points.

However a set of common minimum standards of data security rules and policies should be required to bodies and institutions who wish to participate in the STORK system. This would not only be necessary in order to meet data security state of the art standards expected by such a platform but also support the harmonisation of different security levels of all the players involved in the STORK project. Key action 16 is about "Propose a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector). In the process of establishing an EU regulatory framework on mutual recognition of e-identification and e-authentication based on online 'authentication services' the common minimum standards used by the authentication services that STORK interconnects will be looked at very closely.

At this stage, the transparency of security features of each eID system is based on self-assessment by each Member State based on a template defined by STORK. There is no third-party certification that would provide additional guarantees about the security measures of each system and help other Member States and service providers to define their policy towards these systems.

Conclusion:

Only national assessment is not sufficient for cross-border-data flows. Common minimum standards on data security for the processing of data beyond the core infrastructure of STORK applying to all STORK partners would be desirable. There is a need for guidelines for the service provider explaining why he should use which of the defined 4 levels of "Quality Authentication Assurance" (QAA) for the service he offers. For example it will be required to use the highest level when it comes to request or transfer medical data. Level 4 is the highest level. It requires the use of a qualified certificate. In this context it must be noted that there is not a lack of harmonisation of national frameworks regulating security levels but unfortunately a lack of regulation in most EU member states.

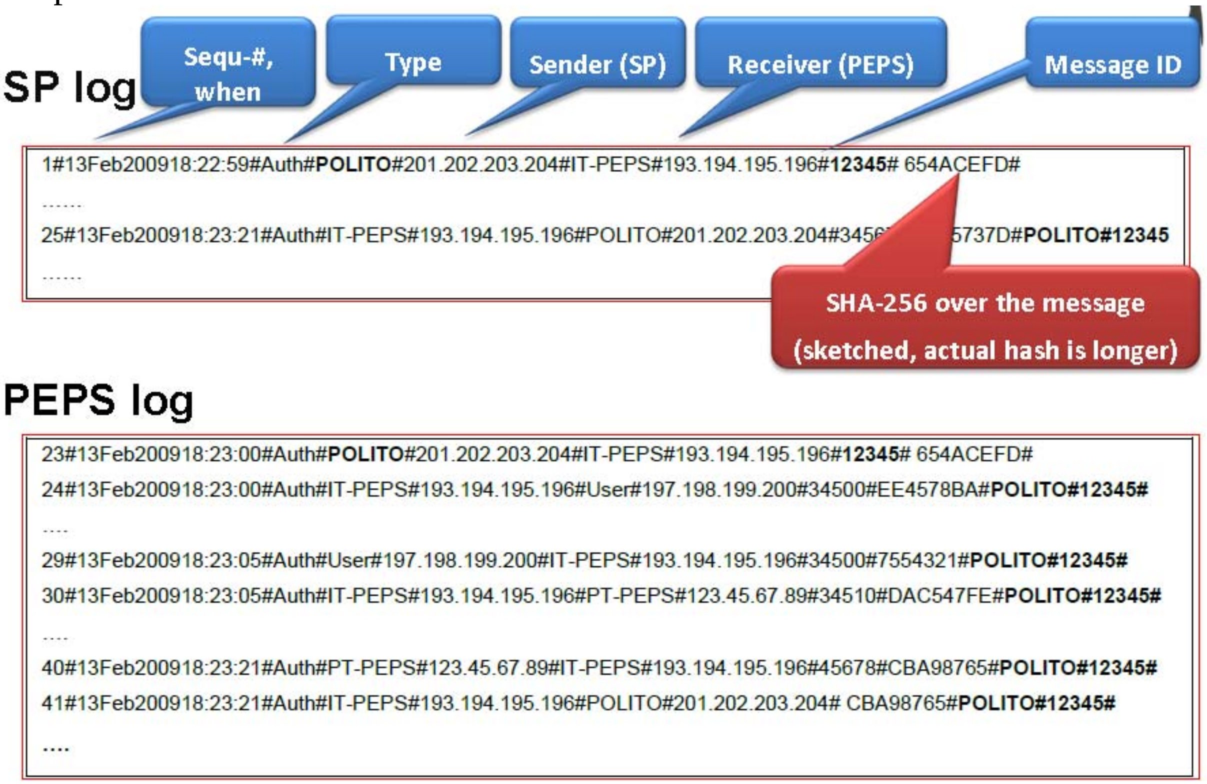
Logfiles created by/in the STORK modules:

Referring to the log-files/traceability chapter of the STORK data protection document a question that came up was what is meant by transaction identification data? Will there be log-files and – if so – which will be retained and for what purpose? Will the IP address and/or the eID be logged?

Conclusion:

To support traceability of each electronic identification process, a hash of the user's data is stored, together with transaction identification data. With this hash the whole transaction can be reconstructed but only with the participation of the user and the service provider. This is a very secure system that makes it very hard to come back to the personal data encrypted this way. However retention/deletion periods should be defined by STORK.

Example:



SP log

```
1#13Feb200918:22:59#Auth#POLITO#201.202.203.204#IT-PEPS#193.194.195.196#12345# 654ACEFD#
……
25#13Feb200918:23:21#Auth#IT-PEPS#193.194.195.196#POLITO#201.202.203.204#3456[illegible]5737D#POLITO#12345
……
```

PEPS log

```
23#13Feb200918:23:00#Auth#POLITO#201.202.203.204#IT-PEPS#193.194.195.196#12345# 654ACEFD#
24#13Feb200918:23:00#Auth#IT-PEPS#193.194.195.196#User#197.198.199.200#34500#EE4578BA#POLITO#12345#
….
29#13Feb200918:23:05#Auth#User#197.198.199.200#IT-PEPS#193.194.195.196#34500#7554321#POLITO#12345#
30#13Feb200918:23:05#Auth#IT-PEPS#193.194.195.196#PT-PEPS#123.45.67.89#34510#DAC547FE#POLITO#12345#
….
40#13Feb200918:23:21#Auth#PT-PEPS#123.45.67.89#IT-PEPS#193.194.195.196#45678#CBA98765#POLITO#12345#
41#13Feb200918:23:21#Auth#IT-PEPS#193.194.195.196#POLITO#201.202.203.204# CBA98765#POLITO#12345#
….
```

Are there revocations lists used in the middleware model?

Conclusion:

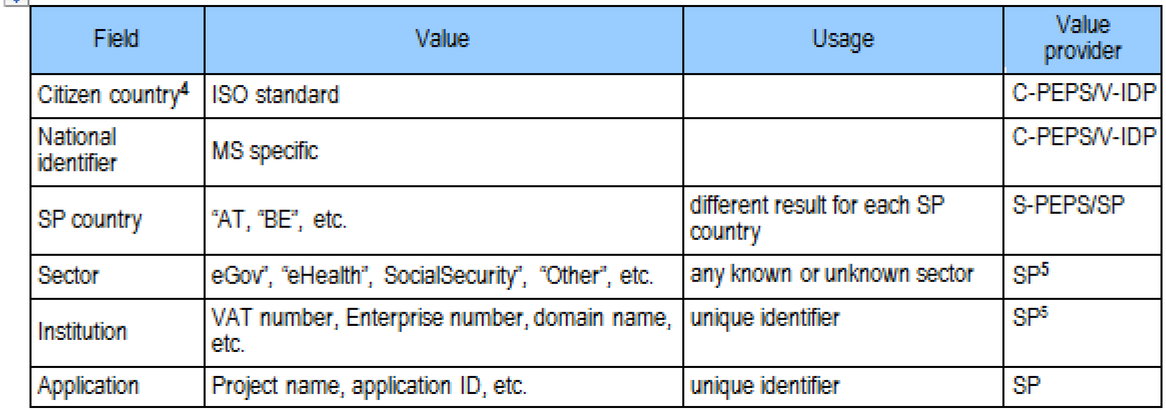
No revocation information in addition to what is legally required out of Annex II of 1999/93/EC (signature directive) is created by STORK.

Hash of personal data

How does the hash-function work exactly? Which entity is in charge of this function? What information is used to set the hash of the users? If there are unique national ID numbers in Member States, will STORK modify or pseudonymise those numbers across countries and sectors in order to prevent a user getting one unique "hash ID" which would make profiling easy.

Conclusion:

In the file that is hashed there are several data. The hash result is therefore not always the same because the data is around the identifier change.



Field	Value	Usage	Value provider
Citizen country[4]	ISO standard		C-PEPS/V-IDP
National identifier	MS specific		C-PEPS/V-IDP
SP country	"AT, "BE", etc.	different result for each SP country	S-PEPS/SP
Sector	eGov", "eHealth", SocialSecurity", "Other", etc.	any known or unknown sector	SP[5]
Institution	VAT number, Enterprise number, domain name, etc.	unique identifier	SP[5]
Application	Project name, application ID, etc.	unique identifier	SP

The national identifier is member state specific. This is entirely up to the MS.
Some MS use the existing identifier (e.g. DNIe in Spain);
Some derive according to their national scheme (e.g. bPK in Austria);
Some derive according to a STORK scheme.

Selective disclosure / data type or data value consent:

Is "selective disclosure" supported by the STORK software: (how) will STORK ensure that only the data which is necessary will be collected and processed (e.g. surname and forename, but not date of birth), thus complying with principle of proportionality and data minimisation? Is it technically possible to select or determine in advance which data shall be read by a STORK partner from an electronic ID card?

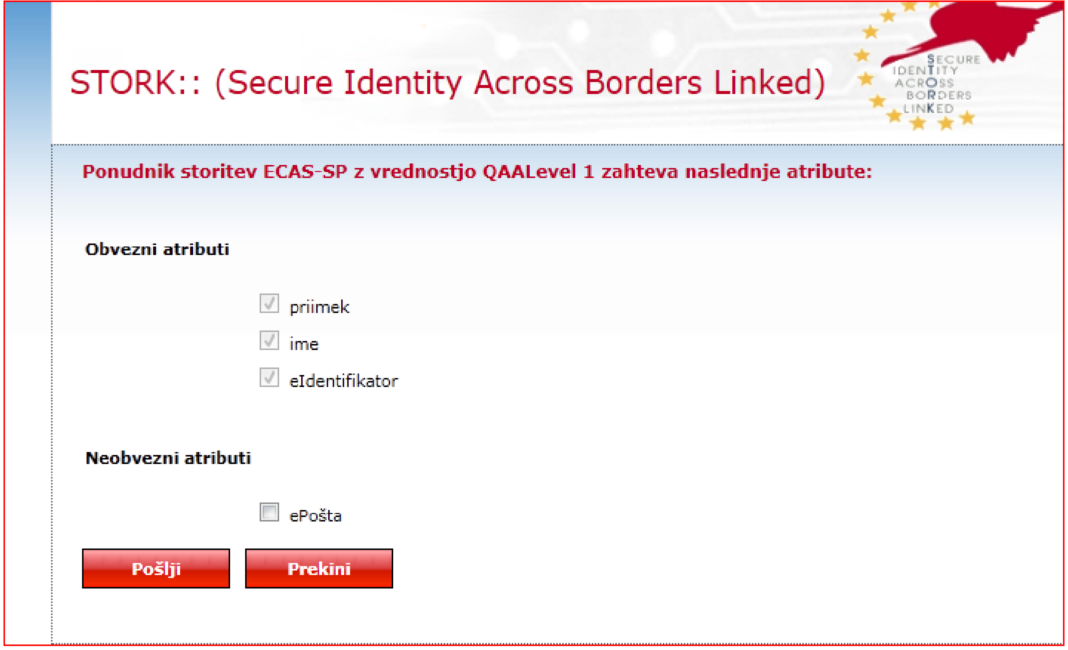
Conclusion:

The Service Provider requests the data he wants/needs in the form of mandatory and optional attributes based on data value or data type consent.
The citizen decides what to send.
STORK does not "negotiate" with SPs what their required attributes are.
The service provider is responsible as controller of the application.

To make it more likely that service provider (SP) will only ask for the data necessary for the service they offer, guidelines should be made available which give specific recommendations how the principles of proportionality and data minimisation in this field should be transposed and taken into consideration by the service provider.

Examples:

Data type consent:



STORK:: (Secure Identity Across Borders Linked)

Ponudnik storitev ECAS-SP z vrednostjo QAALevel 1 zahteva naslednje atribute:

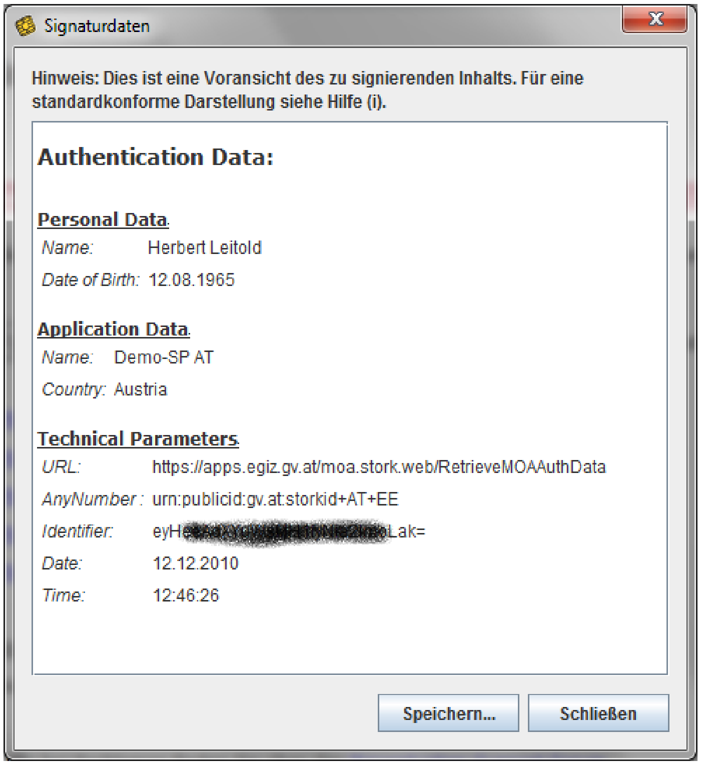
Obvezni atributi

☑ priimek
☑ ime
☑ eIdentifikator

Neobvezni atributi

□ ePošta

Data value consent:



Hinweis: Dies ist eine Voransicht des zu signierenden Inhalts. Für eine standardkonforme Darstellung siehe Hilfe (i).

Authentication Data:

Personal Data

Name: Herbert Leitold
Date of Birth: 12.08.1965

Application Data

Name: Demo-SP AT
Country: Austria

Technical Parameters

URL: https://apps.egiz.gv.at/moa.stork.web/RetrieveMOAAuthData
AnyNumber: urn:publicid:gv.at:storkid+AT+EE
Identifier: eyH[redacted]Lak=
Date: 12.12.2010
Time: 12:46:26

Privacy notice:

Privacy notices explaining what happens with the collected data should be made. They should contain a duty for each SP to explain the necessity of the enquired data in each case. They should be easily accessible. Due to the complex infrastructure created by the 2 different models with all the varieties of data transfers to different applications depending on the citizenship and on the country from which a service is requested from these differences between the specific transactions must be made transparent and understandable. A suggestion would be to create a dedicated privacy note for every possible transaction (e.g. Austria -> Germany; Austria -> Spain,…)

Private entities

Is it planned to open the system for private entities?

Conclusion:

STORK currently addresses mainly eGovernment applications and therefore public entities. Some pilot partners are however private entities.

Examples:
Delivery services in the eDelivery pilot
Schools' (Safer Chat) and also Universities' (Student Mobility) pilots do not fall (completely) into the public/eGovernment area.

As of a draft the CIP (Competitiveness and Innovation Framework Programme) and the ICT-PSP (ICT Policy Support Programme) foresees in the next phase an extension to further sectors, including private entities.

In this context it will be necessary to introduce safeguards that make sure that unique citizen ID numbers may not be shared with private entities in some countries (e.g. Belgium).

Authentication standards:

Some countries, e.g. Germany, will distribute electronic ID-cards that contain a two-way-authentication process (provider -> user and user -> provider). How will mutual recognition of those eID cards with countries other than the origin country be ensured without lowering the level of data security measures?

Conclusion:

The 2 way authentication model can be used by STORK applications:
In the MW model it is provided in the V-IDP or operated by the SP in the "pure MW model" configuration.
In the PEPS model it is provided through mutual authentication with the C-PEPS.
This means however that different standards can be bridged but not compensated. If the partner country has a "lower standard" STORK applications may not raise it.

Sector specific PINs:

If a national system uses a unique eID, how will this ID be treated in the STORK environment and in the participating applications?

Conclusion:

The territorial principle is foreseen.

If the receiving MS uses a cross-sector identifier, the same may be done with received foreign identifiers (which itself may be specifically derived by the sending MS). Example: an Austrian sector-specific ID “bPK” derived for Spain, may be used cross-sector in Spain.

If the receiving MS used sector-specific identifiers, the same applies to foreign identifiers, even used “flat” in home country.
Example: a Spanish DNIe used in Austria is derived sector-specific.

Webdesign:

Will the design and the security certificates on the log-on websites be the same in every country in order to make it easier for the citizens to recognise them and check against fake and fraud websites?

Conclusions:

Recommendations on “look and feel” are made.
Branding and actual integration however is in the SP’s responsibility

For the citizen his “home country eID look and feel” is the familiar one.
E.g. Austrian authenticates against the Spanish PEPS:
He will see the Austrian middleware layout.

Security certificates should come from trusted providers.