Legal evaluation of the FutureTrust architecture

D.5.3

Document Identification	
Date	25/07/2019
Status	Final
Version	1.7

Related WP	WP5	**Document Reference**	D5.3
Related Deliverable(s)	D2.7; D2.8	**Dissemination Level**	PU
Lead Participant	SOTON	**Lead Author**	Niko Tsakalakis
Contributors	Sophie Stalla-Bourdillon	**Reviewers**	Vincent Bouckaert Detlef Hühnlein Mikheil Kapanadze Carl-Markus Piswanger Nuno Ponte

Abstract: The present document performs a Data Protection by Design assessment of the services developed by the FutureTrust project and the pilot and demonstrators designed to test them. This document forms the second iteration of a data protection assessment, with the first performed during the design stage of the FutureTrust services. Following a Data Protection by Design methodology, a brief description is given for each service, pilot and demonstrator, followed by a determination of their stakeholders, data flows, personal data processing and data protection roles. For each, a preliminary assessment of their data protection risk level is performed. The risk level is calculated based on feared events and associated privacy risks for seven categories, and the applied mitigating controls.

1. Executive Summary

This report offers an assessment of the level of data protection for each service designed for the purposes of the FutureTrust project and their implementation during the piloting phase. As such, it should be considered as a preliminary data protection impact assessment.

The FutureTrust project, in line with the GPDR Article 25 Data Protection by Design principle, relies upon an iterative assessment of how the potential operators of FutureTrust services could comply with EU data protection law, with the intention to minimise the risks to the rights and freedoms of the data subjects as early as possible from the design phase.

In order to identify risks, a data protection by design approach was developed right from the start of the project. It consists in translating data protection principles into data protection requirements that can then be implemented or coded within ICT systems. Said otherwise, the data protection principles listed in GDPR Article 5 are translated into data protection objectives or goals, in the sense that the means to achieve these goals will differ from one scenario to another, i.e. from one data environment to another, depending upon the context of the processing and the risks posed to the rights and freedoms of data subjects. Building upon the approach of the German Standard Data Protection Model, seven data protection goals are therefore identified: data minimisation, availability, integrity, confidentiality, unlinkability, transparency and intervenability. For these seven data protection goals control measures are identified and a preliminary risk assessment is conducted based on typical feared events as usually referred in methodologies for data protection impact assessment.

The FutureTrust project therefore relies upon a data protection by design approach that comprises the following steps: a description of the system components and the data flows between these system components for each service, an identification of the potential purposes and legal bases, a description of typical use case, an allocation of roles for each use case, and a preliminary risk assessment based on feared events.

Each FutureTrust service is examined separately. Based on their assessment, the following observations can be made:

- The majority of processing of personal data by FutureTrust services concerns common personal data (see Table 8). The most common category is authentication data (username and password or authentication attestations from eID providers). The IdMS also processes identification data. Where identification data are used within the eIDAS framework, the identification data will consist of the Minimum Dataset. The SigS, the ValS and the PresS process in addition electronic signatures, seals and timestamps and associated electronic certificates. The gTSL only processes e-mail addresses of the users that opt in to the notification feature.
- On occasion, some FutureTrust services might process additional personal data. This might happen in the case of the SigS and the ValS in exceptional circumstances where electronic signatures objects cannot be extracted and parsing of the accompanying electronic document is needed. In these cases, there is a possibility that data contained in a document might belong to the category of sensitive data within the meaning of GDPR Article 9. However, no FutureTrust service is storing said documents or the data contained within.
- In the case of the pilot and demonstrators, additional personal data might be contained within the documents uploaded for validation. The eInvoice application accepts electronic

invoices, the eMandates application accepts electronic mandates and the eApostille application accepts electronic apostilles. Therefore, the electronic invoices and mandates are expected to contain some personal data relating to banking information (account numbers, account owners etc.). The information contained within the electronic apostilles can vary, since in theory a large degree of documents can accept an apostille. However, for testing purposes the type of apostilles that will be accepted is limited and, hence, no sensitive data are expected to be present.

- All personal data are confidential, secured by disk encryption, access control and secure communications (TLS encryption of the communication channels).
- All services validate the integrity of the data, either through the validation of hash values, or through checks with authoritative sources. Where necessary, logging functions have been implemented to assist in auditing the integrity of the data.
- Where additional processing is needed in order to offer added functionalities (such as, for example, the notification feature of the gTSL), the added functionality is offered as an opt in after valid consent.
- Where services can perform their purpose without the need of external datasets, the ability to function in a standalone mode keeps linkability of datasets to a minimum (see, for example, the 'application-centric signing' of the SigS).
- Finally, data minimisation is ensured in all services. Where possible services operate in a stateless mode, where no personal data are stored (Identity Broker in the IdMS, 'pop' operation in the PresS). Where possible, stored data are undergoing pseudonymisation. This happens, for example, for the FIDO authentication data in the IdMS, as well as data held by the SigS, the ValS and the PresS by replacement with hash values.
- When personal data are stored, either decentralised storage (it is the case, for example, in the gTSL Mongo DB or in the IdMS FIDO server) or storage in the control of the user is possible, depending on the implementation.
- Although the data protection by design offered by the FutureTrust services is tested also in an implementation scenario (pilot and demonstrators), it is strongly advised that the organisations incorporating the services perform their own Data Protection Impact Assessments. Since the purposes of an assessment is to assess the risks of processing holistically, taking into account all the technical and organisational elements of an organisation, the present document can only serve as a primer for the 'by design' and 'by default' data protection afforded by the FutureTrust services and greater granularity will be needed to assess the conformity to the GDPR of processing performed in a complex environment.

Consequently, it can be asserted that the FutureTrust services have been engineered to offer 'by design' and 'by default' control measures for all data protection goals and in particular to address three types of feared events: illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data. The processing of personal data taking place in the context of these services is necessary to pursue the potential purposes examined and the advantages derived from the use of these services as designed are not outweighed by disadvantages or negative impacts upon data subjects' rights on the basis of the use cases described. Obviously, the technical controls that have been implemented in the FutureTrust services should be supplemented by organisational and technical measures to be implemented within their broader environments. This document has assessed these types of measures,

pertaining to the rest of the data protection goals, where the FutureTrust services have been implemented in broader environments for the purposes of the pilot and demonstrators. During this assessment, it has been found that the overall technical and organisational measures that complement the implementation of the FutureTrust services mitigate any serious risks to the rights and freedoms of the data subjects and, therefore, the processing operations of the pilot and demonstrators as performed within this project conform to the requirements of the GDPR.

A table summarising the residual risk after all the appropriate safeguards and measures have been applied during the design of the FutureTrust services and the development of the pilots and demonstrators can be found in Table 1.

Data protection goal	***IdMS****	***SigS****	***ValS****	***gTSL****	***PresS****	***eInvoice***	***e-Mandates***	***e-Apostille***	***Smart Certificate***
Purpose limitation	--	--	--	--	--	Low	Low	Low	Low
Legal basis	--	--	--	--	--	Low	Low	Low	Low
Fairness	--	--	--	--	--	Low	Low	Low	Low
Accountability	--	--	--	--	--	Low	Low	Low	Low
Data minimisation	--	--	--	--	--	Low	Low	Low	Low
Storage limitation	--	--	--	--	--	Low	Low	Low	Low
Confidentiality	Low	Low	Low	Low	Low	Low	Low	Low	Low
Accuracy and integrity	Low	Low	Low	Low	Low	Low	Low	Low	Low
Availability	Low	Low	Low	Low	Low	Low	Low	Low	Low
Unlinkability	--	--	--	--	--	Low	Low	Low	Low
Transparency	--	--	--	--	--	Low	Low	Low	Low
Intervenability	--	--	--	--	--	Low	Low	Low	Low

Table 1: Residual risk after applied controls for FutureTrust Services and Pilots/Demonstrators

*Only applicable goals where assessed in the individual Services' assessments, as assessment of the remaining goals is dependent upon the system where the services are integrated into.

2. Document Information

2.1 Contributors

Name	Partner
Niko Tsakalakis (NT)	SOTON
Sophie Stalla-Bourdillon (SSB)	SOTON

2.2 History

Version	Date	Author	Changes
0.1	12/09/2018	NT	Description of FutureTrust services
0.2	07/10/2018	NT	FutureTrust services data protection by design descriptions
0.3	15/10/2018	SSB	Feedback on the descriptions of services
0.4	5/11/2018	NT	Assessment of the data flows, roles and risks
0.5	25/11/2018	NT; SSB	Revision of the assessment on risks and controls; writing up
0.6	30/11/2018	NT	Necessity and proportionality check
0.7	04/12/2018	NT	Revision of gTSL after review
1.0	05/12/2018	NT	Preliminary report on FutureTrust services
1.1	12/02/2019	NT	Description of the pilot and demonstrators
1.2	18/3/2019	NT	Assessment of the data flows and roles of pilot/demonstrators
1.3	22/05/2019	NT	Overall assessment of the risks
1.4	24/05/2019	NT	Format changes
1.5	06/06/2019	SSB	Feedback on assessment of risks
1.6	14/06/2019	NT	Corrections on risk impact tables
1.7	28/07/2019	NT	Feediback from pilots

2.3 Table of Contents

2.4 Table of Figures

2.5 Table of Tables

2.6 Table of Acronyms

CA	Certification Authority
CNIL	Commission nationale de l'informatique et des libertés (French data protection authority)
DB	Database
eID	Electronic Identification
eIDAS	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 [2014] OJ L257/73
EU	European Union
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L119/1
gTSL	FutureTrust Global Trust Service Status List
ICT system	Information and communication technology system
IdMS	FutureTrust Identity Management service
PresS	FutureTrust Scalable Preservation service
SDM	The Standard Data Protection Model
SigS	FutureTrust Remote Signing and Sealing service
SSO	Single Sign On
TLS	Transport Layer Security
TSL	Trust Service Status List
ValS	FutureTrust Comprehensive Validation service

3. Project Description

Against the background of the regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS), the FutureTrust project, which is funded within the EU Framework Programme for Research and Innovation (Horizon 2020) under Grant Agreement No. 700542, aims at supporting the practical implementation of the regulation in Europe and beyond.

For this purpose, the FutureTrust project will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications. In particular, the FutureTrust project will extend the existing European Trust Service Status List (TSL) infrastructure towards a “Global Trust List”, develop a comprehensive Open Source Validation Service as well as a scalable Preservation Service for electronic signatures and seals and will provide components for the eID-based application for qualified certificates across borders, and for the trustworthy creation of remote signatures and seals in a mobile environment.

4. Introduction

This document aims to offer an assessment of data protection requirements for the services designed for the purposes of the FutureTrust project. As such, it should be considered as a preliminary data protection impact assessment. The goal is not to provide a definitive data protection impact assessment, which should instead be performed by the organisations that perform the processing. Instead, the aim is to provide a comprehensive preliminary assessment into the data protection afforded by the FutureTrust services by design, and, the technical controls implemented to mitigate any risks to the rights and freedoms of the data subjects.

Because FutureTrust services are designed to be integrated into other services, the assessment of the level of data protection guaranteed through these services is also dependent upon the environment within which the FutureTrust services will be used. With this said, the FutureTrust project has been deploying a 'by design' approach to data protection, aiming to minimise the risks to the rights and freedoms of the data subjects from the design phase in line with the GPDR Article 25 Data Protection by Design principle.

In this assessment of data protection risks, we therefore only focus on the assets developed by FutureTrust, i.e. the hardware and software modules incorporated in one of the FutureTrust services, and their implementation within the defined pilot and demonstrator environments.[1] The typology of personal data considered refers mostly to common personal data. Sensitive personal data are not outright expected to be processed by the FutureTrust services. Where there is a possibility that sensitive personal data, in the meaning of GDPR Article 9, might be processed by a FutureTrust service, this is highlighted. The same is done when the data processed do not fall under the definition of Article 9, but are perceived as requiring special care, such as for example the processing of social security numbers or bank data.[2]

In order to identify risks, we have followed a data protection by design approach. We have developed a data protection by design approach at the inception of the project, explained in section 5 of this deliverable, which relies upon a systematic examination of 7 data protection goals in order to comprehensively assess the proportionality of the processing. This is because safeguards attached to a processing activity can support the justification of processing. Data minimisation, as the overarching data protection goal, is one area of focus of the examination as it makes it possible to assess necessity of processing activities, i.e. ensuring that the processing activities, the data types and the retention duration are necessary for the purpose of the processing. A second set of data protection goals, i.e. confidentiality, integrity, availability, is also taken into account. As regards unlinkability, transparency and intervenability they are mentioned each time an assessment is possible at the design stage.[3] However, they require a holistic assessment of systems, processes and policies, which becomes possible when the FutureTrust services are operated within their test environments (the pilot and demonstrators of the FutureTrust project). Yet, in the first section of this assessment the FutureTrust services are considered as stand-alone products, without contextual information about practices.

[1] Whereas a complete data protection impact assessment, taking place at the entity incorporating one of the FutureTrust services into their own system, should also look upon other assets, such as the wider information system infrastructure and the supporting organisational assets (e.g. employees, paper processes etc.).
[2] As is the case, for example, with the eInvoices pilot, where banking data are present.
[3] For more information on the data protection goals, see Niko Tsakalakis and Sophie Stalla-Bourdillon, *D2.8 - Documentation of the Legal Foundations of Trust and Trustworthiness* (FutureTrust project, v 1,00, 29 June 2018).

As a result, for the purposes of characterising risks during the assessment of the services, we are considering three categories of feared events: illegitimate access to personal data (confidentiality), unwanted modification of personal data (integrity and accuracy) and disappearance of personal data (availability), as mentioned within data protection impact assessment methodologies.[4] Indeed these feared events could have an impact on all data protection goals. By way of example, unauthorised access would have severe implications when the principle of data minimisation is not engineered, would amount to violations of the principle of purpose limitation, transparency, accountability, could potentially jeopardize the principle of storage limitation, while unwanted modification of personal could have major consequences for the principles of accuracy and integrity and loss of personal data could have a severe impact upon data subjects' ability to exercise their rights. The remaining of data protection goals are not examined for individual services, because their assessment requires contextual information about the integration environment. However, entities considering integrating one of the FutureTrust services can find an assessment of all the data protection goals, that can act as a primer, in the second section of this document.

In the second section of the assessment, the FutureTrust services are examined in context within an implementation environment of the pilot and demonstrators. Although a deeper examination of the surrounding environment, processes and policies of the entity performing the processing is needed for a full data protection impact assessment, which is not feasible in the context of this project, the second section allows the assessment of the designed processing to move beyond the risks of illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data (confidentiality, integrity/accuracy and availability). Feared events and their mitigation controls about data minimisation, unlinkability, transparency and intervenability are checked as well. Further, the assessment looks into the conformity of the pilot and demonstrators to the purpose limitation, legal bases, fairness, accountability, storage limitation, necessity and proportionality principles. Thus, in the second section, where the FutureTrust services are put in context, the full framework for data protection by default is utilised.

Where a likelihood of a feared event is characterised, the intensity of the impact on the rights and freedoms of individuals is then taken into account. The impact can be physical, material or immaterial (moral) and it should be assessed in terms of severity (whether it warrants negligible, limited, significant or maximum infringement upon the individuals affected) and likelihood. For the assessment of the level of impact, the scales of CNIL to estimate severity have been used.[5]

This report thus starts with a description of the data protection by design methodology implemented for the design of FutureTrust services. This description is followed by a description of each FutureTrust service comprising different layers: data flows, processing purposes and

[4] See e.g. CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases* (edition of February, 2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> accessed 25 May 2018, p. 3. See also ICO, *Data Protection Impact Assessments (DPIAs)* (The General Data Protection Regulation: Accountability and Governance, 22 March, 2018) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf> accessed 25 May 2018; CNIL, *Privacy Impact Assessment (PIA): Methodology* (edition of February, 2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf> accessed 25 May 2018; Felix Bieker and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' in Stefan Schiffner and others (eds), *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings* (Springer International Publishing 2016).

[5] CNIL, CNIL, *Privacy Impact Assessment (PIA): Knowledge Bases*, n. 4, pp. 4—5.

potential legal bases, data protection roles per use case and a data protection by design assessment or said otherwise a preliminary risk assessment based on typical feared events.

5. The FutureTrust methodology for data protection by design

Data Protection by Design is a principle introduced by the GDPR. Under GDPR Article 25 the principles of Data Protection by Design and by Default apply, first and foremost, to data controllers.[6] Data processors are indirectly captured by Article 25, in as much as data controllers *"shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures"* as per Article 28(1).

System manufacturers are not directly required to introduce Data Protection by Design in their products, although they are encouraged to do so.[7] However, FutureTrust acknowledges that system manufacturers and engineers often have more control over the *"basic privacy-relevant design decisions"*[8] than controllers or processors have. This is because some design decisions will have an impact upon the means adopted to ultimately reach data protection goals. Effectively this means that Data Protection by Design decisions will be made by producers, i.e. system designers.

Strictly speaking Data Protection by Design and Data Protection by Default should be distinguished. Data Protection by Design is provided for in GDPR Article 25(1) and expresses the obligation of the data controller to *"put in place appropriate technical and organisational measures designed to implement the data protection principles; and integrate safeguards into your processing so that you meet the GDPR's requirements and protect the individual rights."*[9] Data Protection by Default, provided for in GDPR Article 25(2), on the other hand expresses the obligation of the data controllers to *"specify this data before the processing starts, appropriately inform individuals and only process the data [needed] for [the] purpose."*[10] In other words, the two principles operate in parallel: the second principle ensures the capabilities developed as a result of the first principle are activated per default in practice. Hence, both shall be seen as two facets of the same coin and require the engineering of the data protection principles contained in GDPR Article 5: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and, accountability. Importantly, a Data Protection by Design and by Default approach covers both a `data protection-by-policy' and `data protection-by-architecture' approach.[11]

Article 25 is meant to apply before any compliance check is actually needed, since per definition no processing of personal data has actually taken place, although there is an intention on the part of the future data controller to process personal data. It is important to understand that GDPR Article 25 should not be confused with a mere compliance check exercise. To state otherwise would be to make Article 25 purely redundant with GDPR Article 5 to which Article 25 refers. Going

[6] GDPR Art. 25(1): "...the controller shall..."
[7] GDPR Rec. 78: "producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations".
[8] Lee A. Bygrave, 'Hardwiring Privacy' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of the Law and Regulation of Technology* (Oxford University Press 2017), p. 16.
[9] ICO, Guide to the General Data Protection Regulation (1,0,94, 22 March 2018) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 24 May 2018, p. 173.
[10] Ibid.
[11] Sarah Spiekermann and Lorrie Faith Cranor, 'Engineering Privacy' (2009) 35 IEEE Transactions on Software Engineering 67.

beyond Article 5, Article 25 requires the embedding of data protection principles within technology and/or organisational practices. It is therefore crucial to be able to translate data protection principles into data protection requirements that can be implemented or coded within ICT systems. There is thus a link between Data Protection by Design and the formal representation of legal norms.[12] In order to proceed with this implementation or coding it is crucial to understand the normative functions played by the data protection principles:

The data protection principles are intimately related with other provisions of the GDPR, which derive the consequences of the application of said principles in specific contexts. These other provisions should therefore be seen as minimum requirements.[13]

The data protection principles add to these minimum requirements in the sense that they are supposed to still guide the action of data controllers and processors once these minimum requirements have been met, in order to adapt data protection safeguards in relation to the risks posed to the rights and liberties of data subjects by the processing activities at stake. As stated in Article 25 itself it is in the light of the likelihood and severity of *"the risks for the rights and freedoms of natural persons posed by the processing that the means should be selected."*[14]

These data protection principles should be conceived as objectives or goals, in the sense that the means to achieve the goal will differ from one scenario to another, i.e. from one data environment to another,[15] depending upon the context of the processing and the risks posed to the rights and freedoms of data subjects.

We therefore build on the approach proposed by the German Standard Data Protection Model (SDM),[16] which translates data protection principles into data protection goals. In an attempt to connect the requirements of the GDPR to technical and organisational measures, as mandated by Article 25, the SDM organises legal requirements into data protection goals in order to then identify relevant control measures.[17] Seven data protection goals are identified for this purpose: data minimisation, availability, integrity, confidentiality, unlinkability, transparency and intervenability. They are defined in the following way:

- *Data minimisation* is achieved when no or as little as possible data are processed. Processing is considered in relation to the amount of data processed, the number of entities to which these data are disclosed to and the extent of the factual control that these entities exercise over the data. Data minimisation presupposes that the principle of purpose limitation is adhered to, as the necessity of the data is dependent upon the processing purpose.

[12] Dag Wiese Schartum, 'Making privacy by design operative' (2016) 24 International Journal of Law and Information Technology 151.
[13] Felix Bieker and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' in Stefan Schiffner and others (eds), *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings* (Springer International Publishing 2016).
[14] GDPR Art. 25.
[15] Mark Elliot and others, The Anonymisation Decision-Making Framework (UKAN 2016).
[16] Conference of the Independent Data Protection Authorities of eh Bund and the Länder, The Standard Data Protection Model (V1,0 - trial version, March 2017).
[17] "The SDM uses the term 'data protection goals' to describe certain categories of requirements derived from data protection law. These requirements are aimed at properties of lawful processing operations, which have to be ensured by technical and organisational measures." Ibid, p. 9.

- *Confidentiality* refers to the requirement of non-disclosure of certain elements in an ICT system, e.g. input data. In practice, this means that personal data shall only be accessed by authorised users. Confidentiality targets not only unauthorised third-parties, but also actors in the ICT system that do not need to access the personal data for the provision of the service.
- *Integrity* implies that data shall remain unmodified, authentic and correct. This goal requires safeguards for ensuring the accuracy and completeness of the data. Integrity requires both prevention and detection methods. While prevention methods mainly rely upon access-control, detection methods relate to the sub-goal of non-repudiation: the provision of irrefutable evidence that an event or action has occurred.
- *Availability* refers to the requirement of making data accessible, comprehensible and processable. The aim of availability is to ensure that, provided the goal of confidentiality is satisfied, authorised entities have access to the data in a manner and format suitable for the intended processing.
- *Unlinkability* aims to hide the link between two actions, whether the actions correspond to uses, identities or pieces of data. Unlinkability is not expressly referred to in the GDPR. However, unlinkability plays a key role in data protection, as a requirement to satisfy the principles of data minimisation and purpose limitation.
- *Transparency* refers to the necessity of making sure all involved parties are able to comprehend which data are collected, which systems process that data and with what processes and which entities are legally responsible for the processing in relation to a specified processing purpose.
- *Intervenability* aims to ensure that parties to a data processing activity can intervene on the processing activity when needed. Intervenability in a wider sense cover measures implemented by controllers to control the activities of their data processors, or their technical infrastructure.

Although the SDM is helpful in grouping the relevant requirements together, it is important to keep the data protection principles of Article 5 as ultimate targets (see Table 2). The technical and organisational measures employed to meet the data protection goals should be continually assessed at every stage of the life cycle of an ICT system. Although evidently system designers should not be expected to perform an assessment as comprehensive as the one required for data controllers, a preliminary assessment remains possible.

It should be noted that a data protection by design methodology is intrinsically linked with a risk assessment approach.

The French and German Data Protection Impact Assessment methodologies are worth comparing at this stage. They are both based on a preliminary risk assessment, which is however described in different terms. While the German SDM is based on the concept of level of interference, which is derived from the combination of four considerations (*"the purpose of the data processing that is determined by the corresponding legal basis, the level of protection, the duration of storage, the type and the number of possible recipients of the processed data"*)[18] in order to infer the required

[18] Conference of the Independent Data Protection Authorities of eh Bund and the Länder, *The Standard Data Protection Model*, n. 16, p. 33.

level of data protection for the processing at hand (normal, high, very high) and calibrate the appropriate list of controls, the French methodology is based on 5 key questions:[19]

1. Is the purpose specified, explicit and legitimate?
2. Is there a lawful basis that ensures the lawfulness of processing and prohibition of misuse?
3. Is data minimisation performed so that collection and processing are adequate, relevant and limited?
4. Are data accurate and kept up-to-date?
5. Are storage periods limited?

While system designers are not strictly speaking responsible for determining the purposes, basis, and storage periods of the processing, they are tasked with building systems which can include at least two layers of control measures (control measures for systems and control measures for data). Ultimately, they build systems with a range of purposes in mind. It therefore makes sense to conduct a preliminary assessment of the residual risks relating to the feared events relied upon within data protection impact assessment methodologies right from the design stage.

Consequently, a data protection by design methodology is iterative in nature. It should start with a descriptive part in order to identify the system components and the data flows between these system components for each service, the potential purposes and legal bases, the allocation of roles for each use case and a preliminary risk assessment based on typical feared events.

DPP	Lawfulness, fairness and transparency	Purpose Limitation	Data minimisation	Accuracy	Integrity	Storage limitation	Confidentiality	Accountability
SDM goal	Transparency	Unlinkability	Data minimisation	Integrity/Intervenability	Integrity	Data minimisation	Confidentiality	Transparency
GDPR	5(1)(a); 13; 14; 15; 19; 25; 30; 32; 33; 40;42	5(1)(b); 6; 26	5(1)(c); 25; 32	5(1)(d); 13(2)(c); 14(2)(d); 15(1)(e); 16; 17; 18; 20; 21; 25; 32	5(1)(f); 25; 32; 33	5(1)(e); 13; 15; 20; 25; 32	5(1)(f); 25; 28(3)(b); 29; 32	5(2); 7(1); 30; 33(5); 35; 82(3); 83(5)(a)

Table 2: Allocation of SDM goals to Data Protection Principles

[19] CNIL, Privacy Impact Assessment (PIA): Methodology (edition of February, 2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf> accessed 25 May 2018.

The following risk matrix will be used to assess residual risks at the design stage. The matrix is an adaptation from the scales that the CNIL Knowledge Bases provide for the estimation of severity and likelihood.[20]

Severity of impact	Likelihood of threat: Negligible	Limited	Significant	Maximum
Maximum	Medium	Medium	High	High
Significant	Medium	Medium	High	High
Limited	Low	Low	Medium	Medium
Negligible	Low	Low	Medium	Medium

Table 3: Mapping of risks

[20] CNIL, Privacy Impact Assessment (PIA): Knowledge Bases, n. 4, pp. 4—6.

6. FutureTrust services

6.1 Identity Management Service (IdMS)

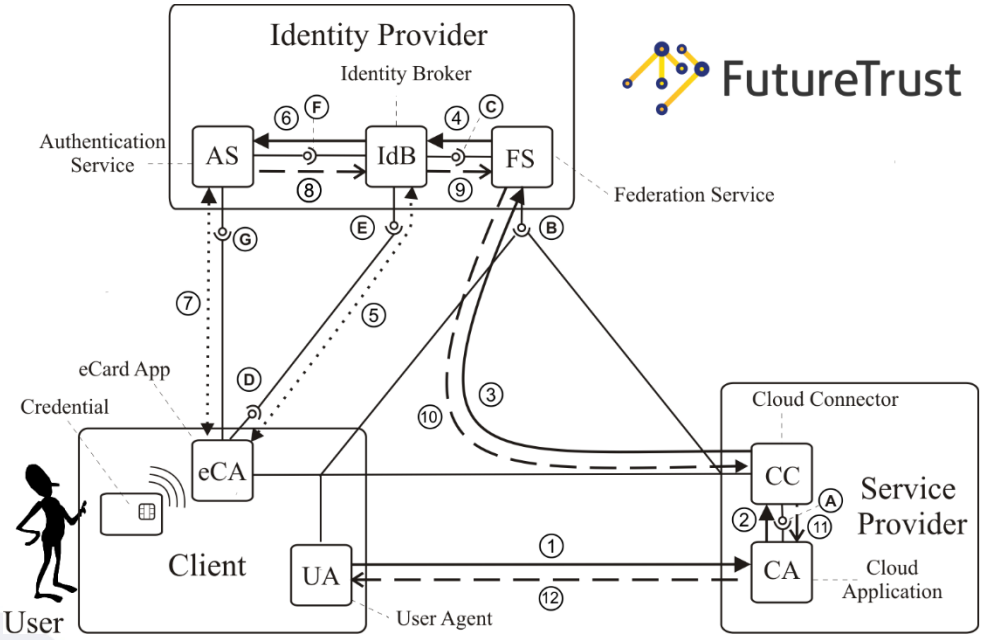


Figure 1: FutureTrust Identity Management Reference Architecture

The FutureTrust IdMS implements the eID service of the eIDAS architecture. The overview of the IdMS is detailed in FutureTrust D3.5.[21] The architecture builds upon a Federated Identity Management model and refines the components of "Client", "Service Provider", which is the party requesting the authentication or identification, and "Identity Provider", which is the party offering the authentication or identification.

For the purposes of this analysis, the "Client" and "Service Provider" components will be black-boxed. Some components of the IdMS are installed on the client and service provider sides, in order for the IdMS to be able to interface with the user and the service provider. In particular, on the user computer an "eCard App" provides access to data held on an eID and a "User Agent" operates in a browser to allow communication with the service and identity providers. The "User Agent" communicates with the service provider via a "Cloud Application" installed on the service provider side. In the same way, the IdMS communicates with the service provider via a "Cloud Connector", also installed at the service provider. Even though these sub-components facilitate or perform processing of data, because they sit and are controlled by the user and the service provider respectfully they are considered out of scope for the present analysis which focuses on the data processing performed by the FutureTrust services.

Below, therefore, the focus will be on the "Identity Provider" component of the IdMS. The term "Identity Provider" is used in the IdMS context to denote a container that encapsulates a number

[21] Detlef Hühnlein and others, *D3.5 Identity Management Service* (Design Documentation, v 1,0, FutureTrust project, 30 May 2017), p. 37—39.

of sub-components: an identity broker that intermediates communication between a (number of) federation services leading to the service providers and a (number of) authentication services. A multitude of authentication services can be supported, from notified national schemes (through eIDAS nodes) to other types of authentication protocols implemented by the various authentication tokens deployed across Europe. The "Identity Provider" component also offers mobile authentication through a FIDO UAF sub-component (which will use the identity broker of the IdMS for user registration/deregistration).

6.1.1 Stakeholders

D3.5 does not explicitly identify all involved stakeholders in IdMS, perhaps because IdMS is designed to be integrated into an (unknown) multitude of services. However, basic categories of stakeholders can be derived from the "Stakeholder Requirements" section.[22] D3.5 explains that the business purpose of the IdMS is to "*enabl[e] citizens and Service Providers to use eID cards for remote electronic identification. In addition, the IdMS enables the derivation of credentials from ID cards for mobile authentication […] in particular using the FIDO UAF protocol.*"[23]

From the above we can derive that the stakeholders involved in IdMS are at least (a) the citizens wishing to authenticate to an online service, (b) service providers providing online services requiring authentication, (c) the FIDO UAF service deriving credentials from eIDs and providing mobile authentication; the FIDO UAF service can reside at the same entity operating the IdMS or operate as an external service the IdMS connects to. To those an additional category should be added, (d) the identity providers (i.e. in the case of EU Member States, the notified national schemes, denoted as 'authentication providers' in the figure above) who operate the authentication of eIDs, from which the citizens will either directly authenticate against services or derive their credentials for FIDO.

It is unclear whether the IdMS in its entirety (denoted in the figure above as 'Identity Provider') or its sub-components – the identity broker and federation service – should also be considered as stakeholders. However, considering these components most likely perform some form of processing of data, it would be prudent to do so.

6.1.2 Data flows

According to Figure 1, the typical journey for a successful authentication involves the steps below:

1) The citizen requests access to a service through a user agent (browser) (Fig. 1, (1));
2) The cloud application installed at the service provider receives the request and forwards to the cloud connector who relays the request to the identity provider through the federation service (Fig. (2,3));
3) The federation service notifies the identity broker for the request; the identity broker then requests that the citizen indicates their authentication provider (Fig. 1, (5));
4) The identity broker forwards the request to the selected authentication provider (fig. 1, (6)) and the authentication provider performs the authentication through the citizen's eCard App (fig. 1, (7));

[22] Hühnlein and others, *D3.5 Identity Management Service, n.* 21, p. 40.
[23] Ibid.

5) If the citizen is performing an identification through an eID card, the identification happens at this stage and the authentication provider forwards the attestation of the identification to the identity broker, which then relays it to the federation service and the cloud connector (fig. 1, (8, 9, 10)); if the citizen is using a third-party identity provider, then the authentication provider forwards the authentication to the identity provider who then relays an identification attestation to the identity broker. The identification attestation is forwarded by the federation service to the cloud connector.
6) The cloud connector relays the attestation to the cloud application, which then grants access to the citizen (fig. 1, (11, 12)).

As aforementioned, the client and service provider side will be considered black-boxed (fig. 1, steps 1-2, 7 and 11-12) and hence out of scope of the present analysis.

6.1.3 Processing purposes and legal bases

As already indicated the general purpose of the IdMS is to ease the electronic identification by combining electronic identification against several authentication providers under a common umbrella.

However, since the IdMS is not a standalone service, but rather it is meant to be integrated into the workflow of other services (e.g. third parties interfacing with eID providers or eIDAS nodes operated by Member States), the purposes for the processing of personal data should be determined according to the purposes of the entity integrating an IdMS.

Inevitably, the integrating service will be the one that will define the appropriate legal bases according to the purposes of processing. Determining the legal bases without knowledge of where the IdMS will be implemented is premature. It is likely that the basis might be based on task carried out in the public interest or legitimate interests of the controller, where the purpose is to satisfy security requirements for accessing an eGovernment service or compliance with a legal obligation of the authentication provider.[24] On occasion, processing might be based on the performance of a contract,[25] if private entities participate in the authentication process (as, for example, in the case of the national scheme in the UK where private identity providers have contractual relationships with the public-sector identity broker).

It should also be mentioned that there are several points in the data flow described above where more than one entities are processing personal data. For example, where the citizen is relying on a third-party identity provider (i.e. a national scheme performs the identification) and the citizen is using FIDO to authenticate, both the FIDO component and the identity provider will be processing data. In cases like these, each entity should obviously operate under its own legitimate basis.

6.1.4 Personal data processing use cases

Several processing activities can be distinguished in the data flow above. D3.5 identifies four categories of activities.[26] Below we provide selected use cases for the four activities.

[24] GDPR Art. 6(1)(c).
[25] GDPR Art. 6(1)(b).
[26] Hühnlein and others, *D3.5 Identity Management Service, n.* 21, pp. 43—46.

6.1.4.1 Identification and authentication

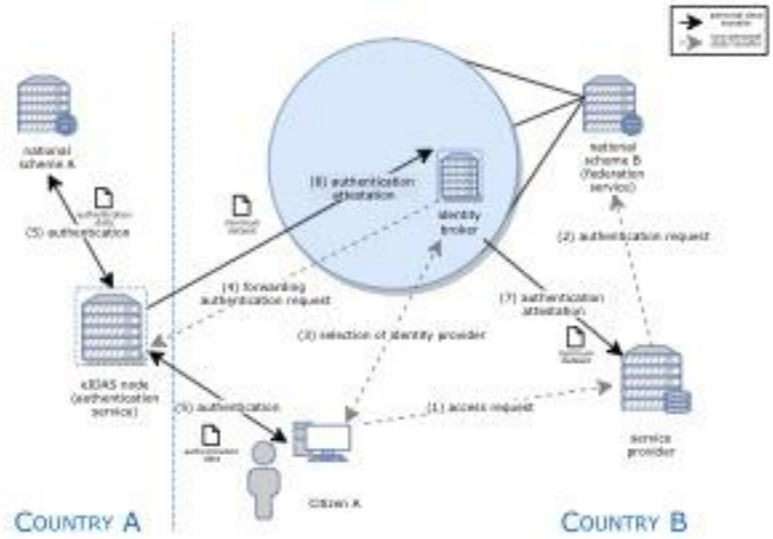


Figure 2: Identification and authentication use case (in relation to data flows)

A citizen of country A, residing in country B, wishes to authenticate against the tax authority of country B, where they claim their annual taxable income. The tax authority of country B wants to identify the citizen so that the citizen will be able to declare their taxable income for the current year and add it to the declared income of the previous years.

The tax authority sends a request for authentication to the national scheme (also in country B). The national scheme of country B, using the IdMS identity broker asks the citizen to present their eID card to the card reader connected to the citizen's computer. The citizen connects their card with the card reader. The IdMS identity broker recognises the card as belonging to the national scheme of country A.

The IdMS identity broker redirects to the (notified) national scheme of country A, operated as an eIDAS node in proxy mode in the territory of country A by the operator of the national scheme of country A. The national scheme reads the data from the card of the citizen and signs an attestation that includes the citizen's minimum dataset (name, date of birth, unique identifier). The national scheme of country A might or might not present to the citizen a confirmation dialogue that the minimum dataset will be sent to the service provider.

The attestation is sent to the identity broker who then forwards it through the federation service to the tax authorities of country B. The national scheme of country B (the identity provider operating the IdMS) might or might not present the citizen with a confirmation dialogue that their minimum dataset will be sent to the tax authorities of country B.

The minimum dataset reaches the tax authorities of country B, where it is matched against a local account of a tax subject with the same name and date of birth. The unique identifier is associated with the local identifier used to identify the user account. The tax authorities present the citizen with the record they hold for them and allow them to declare a taxable income for the current financial year.

6.1.4.2 Credential derivation and FIDO registration

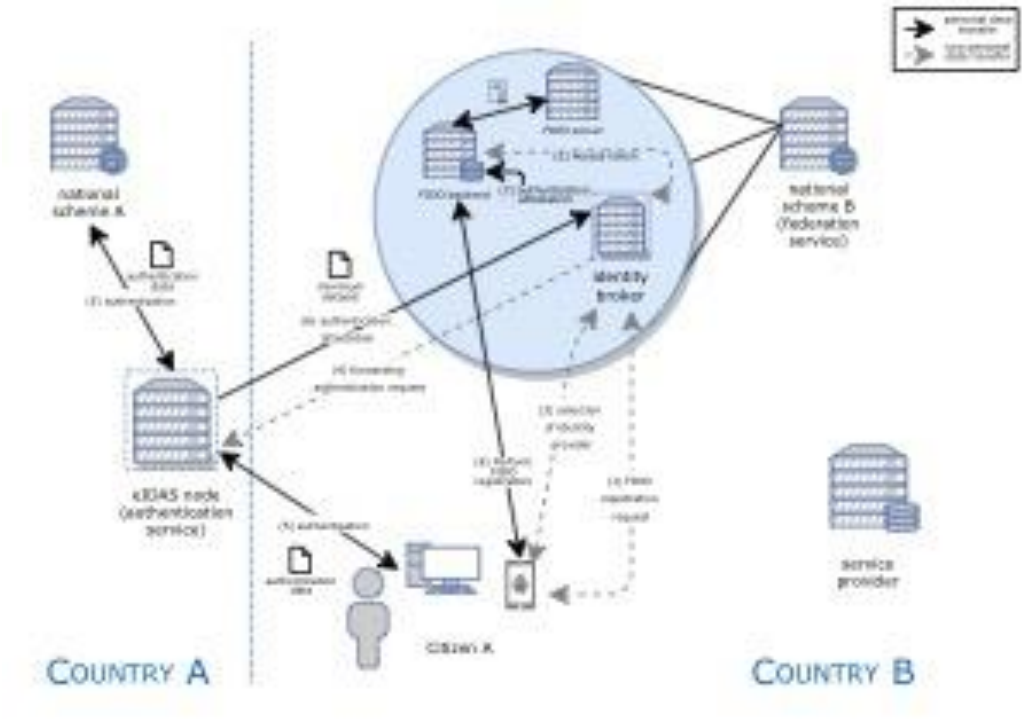


Figure 3: FIDO registration (in relation to data flows)

A citizen of country A residing in country B wishes to access an online service in country B using a mobile token. The citizen asks to access the service of country B. The service requests an authentication to the national scheme of country B. The national scheme of country B, using the IdMS identity broker asks the citizen to signify how they want to authenticate. The citizen selects mobile FIDO authentication. The identity broker asks the citizen to login or register. The citizen selects the registration button. The identity broker redirects to the national scheme of country A, where the citizen authenticates using their eID card (following the same process as outlined in the example above). The signed attestation is forwarded by the national scheme of country A to the identity broker in country B. The identity broker redirects to the FIDO UAF service. The FIDO UAF service generates a 2D barcode which is displayed in the citizen's computer. The citizen scans the 2D barcode with their mobile device. The citizen authenticates to the FIDO UAF with the 2D barcode using their mobile device. The citizen registers their FIDO UAF public key and the FIDO authenticator attestation (if available) at the FIDO UAF service. The FIDO UAF service creates a pseudonymous unique user ID and a pseudonymous unique key pair, that is pairwise persistent between the identity provider and the user. The FIDO UAF service issues a certificate for the key and the data retrieved from the attestation (in essence linking the FIDO credentials to eID data), stores it in a hardware security module either in the FIDO backend or at the citizen's computer[27] and redirects it to the citizen.

[27] Andreas Chalupar, *D4.6 - Identity Management Service* (draft v 0,03, FutureTrust project, 10 July 2018), p 12.

6.1.4.3 FIDO authentication

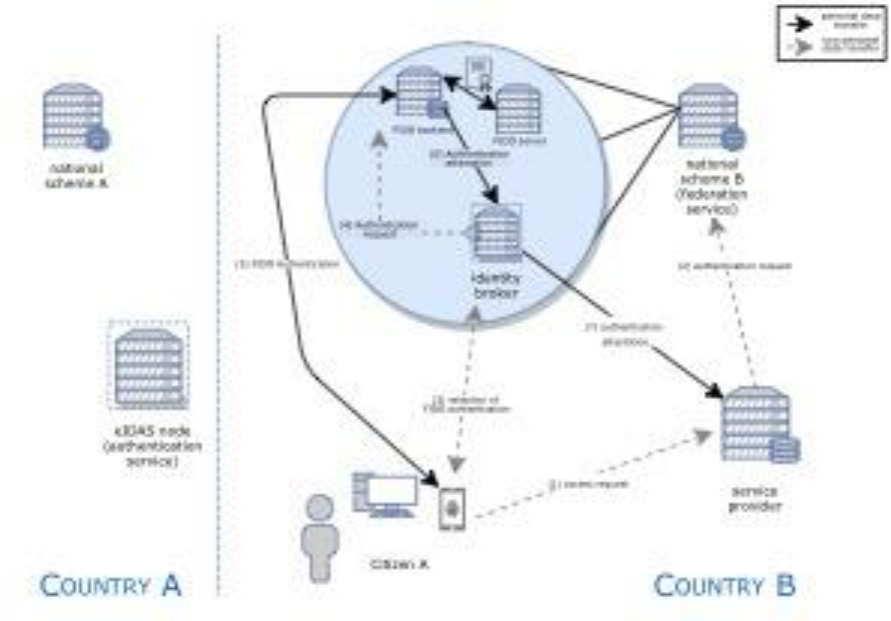


Figure 4: FIDO authentication (in relation to data flows)

This example continues the process started in 4.1.4.2 after the citizen is provided with a valid certificate from the FIDO UAF service (FIDO registration). After successful registration, subsequent authentication to the citizen's identification provider, in order to produce attestations for service providers, can happen through the use of the citizen's FIDO credentials. This allows for mobile authentication, even if the identity providers themselves do not support it, as well as pseudonymous authentications, since the FIDO credentials are pseudonymous attributes. The identity broker forwards the authentication request received by the service of country B to the FIDO UAF service. The FIDO UAF service asks the citizen to authenticate using their FIDO UAF key pair and their mobile phone. Upon successful authentication, the FIDO UAF service redirects to the identity broker along with the certificate containing the link between the FIDO credentials and the identification data.[28] The broker sends the authentication, containing the certificate, containing eID data (in an eIDAS context the minimum dataset) of the citizen to the service of country B through the federation services. The broker does not store the data. The service matches the minimum dataset to a local account and grants access to the citizen to this local account.

In case the eID data are not derived from an eID card located at the citizen's computer (in other words, in schemes where the identity provider is a separate entity not under the control of the user), then the eID data are sourced from that separate entity and forwarded to the service through the identity broker.

[28] Ibid, p. 16.

6.1.4.4 FIDO deregistration

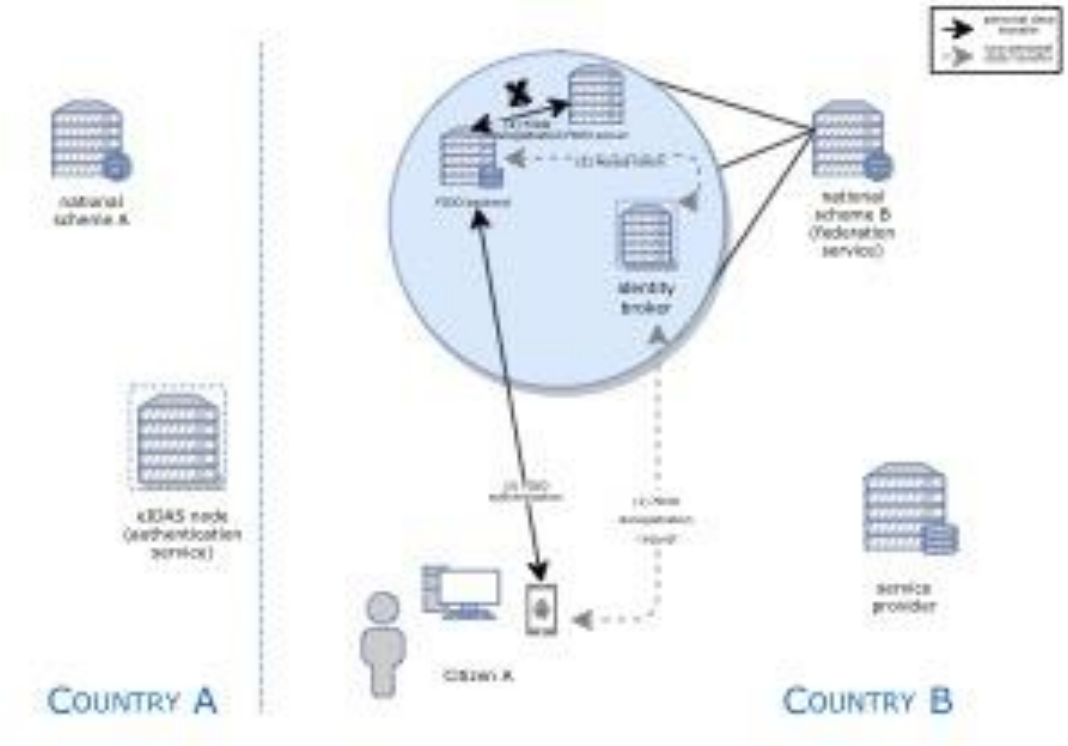


Figure 5: FIDO deregistration (in relation to data flows)

The citizen of country A wants to deregister a FIDO UAF key pair from the identity provider of country B. The citizen requests the deregistration from the national scheme of country B. The national scheme using the identity broker forwards the request to the FIDO UAF service. The FIDO UAF service confirms with the citizen that they want to deregister (through authentication). The FIDO UAF service deletes the citizen's public FIDO key. The identity broker deletes the link between the FIDO credentials and the eID data of the citizen's identity provider.

6.1.5 Data protection roles per use case

On the basis of the use cases described above, we can distinguish the data protection roles that each actor in the FutureTrust IdMS ecosystem plays.

The three roles of interest for data protection are:

- The **data controller**: "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;*"[29]
- The **data processor**: "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*"[30]

[29] GDPR Art. 4(7).
[30] GDPR Art. 4(8).

- The **data subject**: "*an identified or identifiable natural person*".[31]

6.1.5.1 Identification and authentication

In this scenario, in the example of cross-border identification, the main actors are the user, the service provider in question, i.e. the party requesting the authentication or identification, the operator of the national scheme of country A, the operator of the national scheme of country B and the IdMS. The IdMS is positioned at the operator of the national scheme of country B, or a separate entity interfacing with the national scheme of country B. The purpose of this data flow is to provide authentication to a citizen requesting access to a service.

The service provider processes the personal data of the user that are already associated with the user's local record (for example a user's tax record). However, this processing is out of scope for this deliverable, as it does not concern data that are transmitted through the FutureTrust services. Instead, **the service provider should be considered a data controller because it requests (and processes) the personal data received as part of the authentication process in order to match the eID of the user to a local record** (the minimum dataset, step 7 of fig. 2 above).

In the same respect, the operator of the national scheme of country A (the citizen's country of origin) is a controller because it determines the personal data processed for the registration and use of the eID of the user (i.e. when issuing a new eID means). However, this processing is again out of scope as it is performed prior to the authentication and/or identification against a service through the IdMS.

In the authentication data flow, the operator of the national scheme receives a request from the service provider to perform an authentication and return the result to the service provider. **The operator of the national scheme of country A should be considered a controller** in its own right because it maintains a separate relationship with the user than the relationship the service provider has with the user. It is a question whether the identity provider and the service provider should be considered as acting towards the same processing purpose (i.e. to authenticate a user to a service) and, therefore, are joint controllers or are acting towards different purposes (the purpose of the controller is to offer authentication services and the purpose of the service provider to consume authentication services) and should be considered as data controllers in common. There is an argument that for the data in transit between the identity provider and the service provider during authentication or identification, the relationship should be viewed as a joint controllership.

The IdMS (the federation service, the identity broker and the selected authentication service) do not in themselves determine processing purposes. They instead perform processing in the form of relaying information from the service and identity providers, on behalf of the service and identity providers (steps 6 and 7, fig. 2 above). **The IdMS should, therefore, be considered as a processor** on behalf of the service provider and the national scheme A. If the IdMS is located at the national scheme of country B, then that national scheme will act as a data processor on behalf of the service provider and the scheme of country A. If the IdMS is a third-party entity, interfacing with the national scheme of country B, then the national scheme of country B will be a data processor and the entity operating the IdMS its sub-processor. In case the entity operating the IdMS does not interface with the scheme of country B at all, the scheme of country B does not have a data protection role in the dataflow.

[31] GDPR Art. 4(1).

Finally, the user (the citizen) is providing the authentication data, and has originally provided the identification data for the eID at their national scheme. The user, in other words, is the data subject.

6.1.5.2 FIDO registration

In this scenario, the main actors are the user, the entity where the IdMS and FIDO UAF reside (for example the national scheme of country B) and the operator of the national scheme of country A. If the FIDO UAF service is a third-party service that interfaces with the IdMS, then that service should be considered as a separate entity. The purpose is to allow a user to authenticate in the future against services through their mobile device, by associating their mobile device with their authentication data.

The entity controlling the means and purposes for the FIDO registration is the FIDO UAF service (with its sub-components, the FIDO back-end and the FIDO server). The FIDO UAF service is producing a certificate linking an eID attestation to the user's key, storing the certificate to the FIDO server or the user's phone. Therefore, **the FIDO UAF should be considered a data controller** (steps 4, 7 and 8 of fig. 3). In case the FIDO service is situated within the IdMS, the entity operating the IdMS is the data controller.

In case the FIDO UAF service is a separate entity, interfacing with the IdMS, the IdMS' identity broker, used to relay the user's access token and the authentication attestation from the national scheme to the FIDO UAF service, should be considered **a data processor on behalf of the entity operating the FIDO UAF scheme** (steps 2, 4, 6 and 7 of fig. 3).

For the national scheme of country A what was explained above holds true. In this scenario, the scheme is in charge of acquiring the user's authentication data and producing the attestation for the FIDO UAF service. Therefore, **the national scheme should be considered as a data controller** along with the FIDO UAF service (steps 5 and 6, fig. 3).

The user is the data subject.

6.1.5.3 FIDO authentication

The main actors here are the user, the service provider requesting the authentication, the FIDO UAF service and the operator of the national scheme of country A. The purpose of this data flow is to authenticate the user against their identity provider using their FIDO credentials, in order for the identity provider to provide an eID attestation to a service provider.

The service provider is a data controller, in line with what was explained in 6.1.5.1 (steps 2 and 7, fig. 4).

The FIDO UAF service performs the authentication of the user, selects the key pair and sends it back to the identity broker. It can be argued that in this case the FIDO UAF service acts as a joint controller with the service provider, since it checks if there is an existing key pair associated with the user's phone and sends that key pair back to broker (steps 5 and 6, fig. 4). However, in line with what was previously explained about the role of identity providers, the FIDO service is processing data for the purpose of authenticating the user so that their identification data can be sent to the service provider. Therefore, it would make sense to consider **the FIDO UAF service processes data as a data controller**.

The citizen's identity provider (e.g. the national scheme of country A) provides the eID attestation. **The identity provider**, hence, should be seen as **a data controller**.

The identity broker, relaying data in steps 3, 4, 6 and 7 of fig. 4, **acts as a data processor** on behalf of the service provider.

The user is the data subject.

6.1.5.4 FIDO deregistration

In this scenario only the user, the identity broker and the FIDO UAF service are involved. The purpose of the flow is to allow users to request the deletion of their associated credentials from the IdMS.

The FIDO UAF service acts as a data controller (in the same capacity as in 6.1.5.2), who conforms to the user's right to erase their data.

The user is the data subject exercising their rights in respect to data erasure and objection to processing.

The identity broker acts as a data processor, in steps 1 and 2 of fig. 5, passing on the request of the user and the access token to the FIDO UAF service.

6.1.6 Data protection by design in the IdMS

The purpose of the IdMS is to offer authentication and identification by connecting several authentication services through an identity broker. As such the IdMS will be processing two main categories of data: authentication data and identification data. Authentication data might be dependent upon a third-party identity provider (for example, a national scheme of a foreign country) or might be authentication data created by the FIDO service. However, in both cases they should be considered personal data, since they are unique information that can make an individual identified or identifiable. The identification data, however, at least in an eIDAS setting will comprise the minimum dataset as defined by eIDAS (at the very least a first and last name, date of birth and unique identifier and in cases previous name(s), current and previous address(es)).[32]

Notably, the data protection afforded to these data will also depend on the choices of the data sources, i.e. the safeguards implemented at the citizens' identity providers. Since the IdMS is designed to act as a broker between the service provider and the identity provider, it will inherit the protections (and risks) of the systems it is interfacing with. Nonetheless, the IdMS shall ensure the protection of personal data it processes both in transit and at rest.

Confidentiality risks can result in the unauthorised disclosure of personal data, which can in turn enable profiling of the data subject or even identity theft. In transit data are protected against illegitimate access (confidentiality) through the deployment of standardised protocols (OpenID, SAML2.0) and the encryption of the transmission channels through TLS. Additionally, transmission takes place only after mutual authentication between the sub-modules (the identity broker, the authentication and federation modules) through access tokens. Access control is implemented by default, since authentication is needed in order to derive identification credentials and when using the FIDO service two-factor authentication is in place.

There are minimal cases where personal data are preserved at rest. The ID broker module is configured for a stateless operation, without the need to save personal data. Where a link between the FIDO key pair and identification data are saved (in the form of a certificate), the saving location can be positioned at the sphere of the citizen. If the saving position (a FIDO server) is however

[32] Implementing Regulation 2015/1501, ANNEX.

positioned at the IdMS, the confidentiality of at rest authentication keys is protected cryptographically. Data storing is performed in a hardware security module.

Unwanted modification of the data could result in invalid data or data that are valid but do not represent the data subject. In such cases, risks of authentication and identification mismatches arise, which would lead to the user being denied access to a service or a user being granted access to an incorrect user account (amounting to identity theft). The **integrity** of the data against unwanted modification is maintained by validity checks against the issuing certification authorities and the integrity of the data exchanges is checked through validation of the access tokens.

Where the **availability** of the data is threatened, a potential disappearance of personal data could generate errors and malfunctions, prohibit access to the service or provide a different service than the one expected. Since the ID broker is stateless, availability of data (protection against the disappearance of data) depends upon the authentication and identification provider. Where the identity credentials are derived from a smart-card in the possession of the citizen, it is assumed that availability of the data is a non-issue; where a third-party provides the identification credentials, their availability will depend on the third-party's internal processes (back-ups of the data, back-up transmission channels in case of down time). Where FIDO credentials are used, the user (the citizen) has the option to store these credentials locally, so that their availability is secured against inaccessibility of third party services; if the credentials are stored with a third party (either in a FIDO server in the IdMS or a third entity) similar processes as in the case of third party identification providers should exist to ensure reachability and availability of the data.

Finally, when the IdMS is creating authentication credentials (through FIDO) it minimises the data processed (**data minimisation**) by constructing pairwise-persistent pseudonymous keys and the citizen's self-defined password is transmitted in a hashed value.

We should note that, although **unlinkability, transparency and intervenability** cannot be fully assessed in pre-production, the IdMS has implemented steps to assist in meeting these goals. A degree of linkability is essential to the nature of the service, as matching of some data is needed to perform identification. However, the IdMS minimises the risks of excessive linkability, which could potentially allow for the profiling of the data subjects, by implementing an identity broker that processes data only in transit without a need to store them and by pseudonymising the credentials used for FIDO authentication. The transparency of the processing performed by the IdMS is ensured through the prompts shown to the data subject: identification through an identity provider is performed only after an active choice of the citizen from a list of potential providers and the eID client situated at the citizen's computer presents the citizen with a list of the required personal data prior to their transmission. Finally, the exercise of data subject rights (intervenability) is established for those components operated by the IdMS (namely, the FIDO UAF service) through the provision of the FIDO deregistration data flow. It is expected that corresponding processes will be followed by the identity and service providers the IdMS will interface with.

As a consequence, adopting a risk-based approach and focusing upon the three following feared events as per CNIL methodology[33], illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data, we obtain the following assessment (*see* the Appendix in section **Fehler! Verweisquelle konnte nicht gefunden werden.** for the complete r isk matrix including an evaluation of risks before applying controls):

[33] CNIL, Privacy Impact Assessment (PIA): Knowledge Bases, n. 4, p.3.

Feared event	*Levels of severity/likelihood*	*Control measure*	*Residual risk*
Illegitimate access to personal data (confidentiality)	Significant	Disk encryption; TLS; session tokens; access control; stateless operation	Low
Unwanted modification of personal data (accuracy and integrity)	Significant	Access control; validity checks; session tokens	Low
Disappearance of personal data (availability)	Significant	Federation and authentication services; FIDO credentials stored locally	Low

Table 4: Controls and residual risks in the IdMS

Since the purpose of the IdMS is to facilitate authentication and identification, the processing of identification and authentication data is necessary. No further data are processed and the authentication and identification data are relayed from the authentication services to the service providers and not stored in the identity broker. Processing of only the identification and authentication data is adequate and directly relevant to the purpose.

Additionally, no further limitations are imposed on the data subjects than the limitations already imposed when the data subjects use their identity providers; instead, use of the IdMS provides the data subjects with additional benefits by increasing the number of service providers that can accept their electronic identity.

As a result, it can be claimed that processing in the IdMS satisfies the **necessity** and **proportionality** principles.

6.2 Remote Signing and Sealing (SigS)

The SigS service aims at materialising the signature-related part of eIDAS, by allowing users to create electronic signatures and seals using local and remote signature creation devices. On top of the Qualified Signature Creation Devices, defined by eIDAS,[34] the SigS also supports signature cards.

The SigS is designed as a software component that can be integrated in application systems. The SigS supports local creation of electronic signatures and seals when a signature creation device is attached to the computer or supports remote creation of electronic signatures and seals by communicating with remote signing services (Trust service providers).

6.2.1 Stakeholders

The SigS is a software component that will reside at the computer of the user. As a result, the main stakeholder will be the user, i.e. the person creating and using electronic signature and seals. In order to create electronic signature and seals, the SigS communicates with external services. Therefore, additional stakeholders should be considered the electronic identity provider that provides authentication services to the SigS and the certification authority that creates the corresponding electronic certificates for the electronic signatures and seals.

6.2.2 Data flows

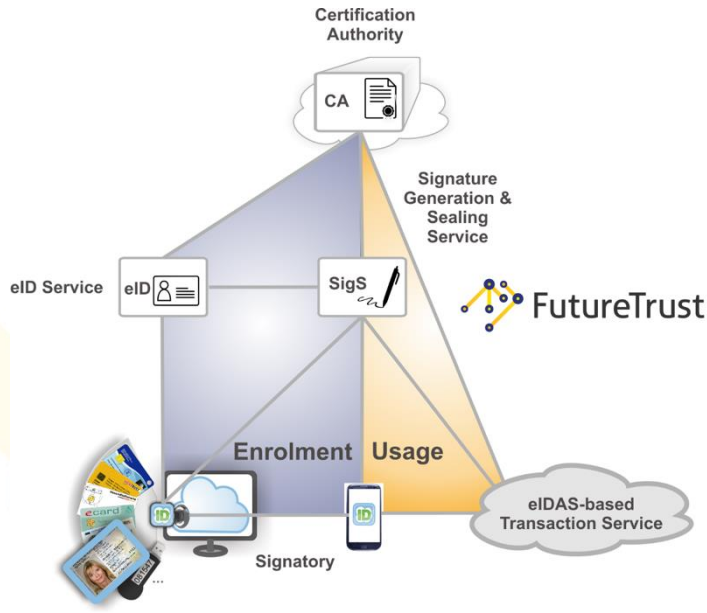


Figure 6: Overview of The SigS

As can be seen from the high-level diagram of the SigS,[35] the service has two phases: the enrolment phase and the usage phase. During the enrolment, the user registers at the SigS through an eID-based identification using their eID and the appropriate eID service (i.e. national

[34] eIDAS Art. 3(23).
[35] Deliverable D3.6, p. 8.

eID scheme). However, the data flows for the eID-based identification are considered out of scope for this analysis. In case the electronic identification happens using FutureTrust's IdMS, what was detailed in 6.1.2 applies.

In order to be able to create electronic signatures and seals, the user requests a registration in the SigS. The SigS redirects the user to their selected eID service (e.g. national eID scheme) where the user authenticates. The eID service sends the SigS an attestation of the identification of the user. The SigS uses this attestation to create a key pair and then requests a Certification Authority for a certificate.[36] The SigS then issues to the user credentials to be able to use the service and an access token for use with their mobile device.

Usage of the service can have different data flows depending on the topology where the SigS is installed. In a high level, the user will access the SigS through the issued credentials. They will select a document for electronic signing or sealing and send it to the SigS. The SigS will use the user's credentials to activate the user's private key, create an electronic signature and apply it to the document. The signed document will either return to the user or be sent off to a third party. Although this describes the overall process, the data flow and the components involved slightly change depending on the deployment of the SigS on the user's system. This is because the SigS is designed to support both local and remote storage.[37] This will be analysed below through the use cases.

6.2.3 Processing purposes and legal bases

As highlighted in the overview of IdMS, the analysis of processing purposes and legal bases here is indicative and a thorough examination should be performed when the FutureTrust services are deployed to the host systems.

However, in general the SigS is processing data in order to allow for the creation and use of electronic signatures and seals that will be embedded into other objects, i.e. in electronic documents. In terms of legal bases, again several may be applicable, although after eIDAS and its requirements for electronic signatures and seals, compliance with a legal obligation might be considered the most appropriate.[38]

[36] Detlef Hühnlein and others, D3.6 Remote Signing and Sealing (Design Documentation, v1,0, FutureTrust project, 31 May 2017), p. 8; ibid, p. 15: "The Enrolment API allows to trigger an enrolment process in which the SigS engages in a protocol with an external Certification Authority (CA) in order to obtain a certificate, which can be used for subsequent signing or sealing processes."
[37] Ibid, p. 11.
[38] GDPR Art. 6(1)(c).

6.2.4 Personal data processing use cases

6.2.4.1 eID-based enrolment[39]

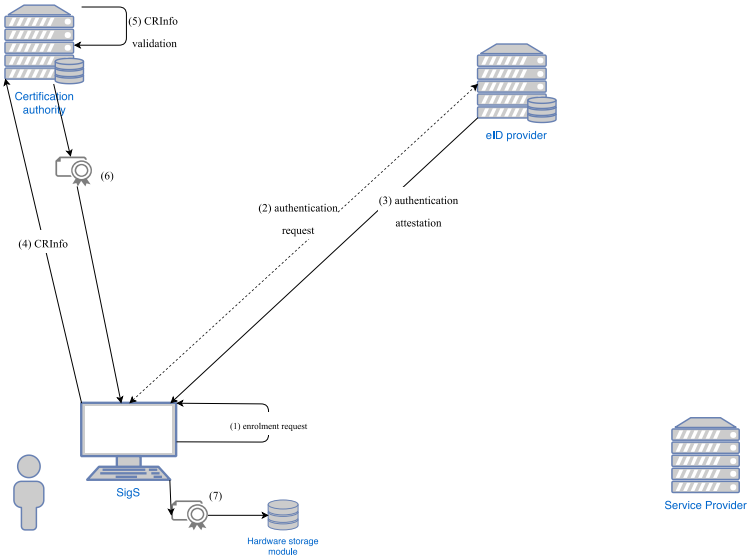


Figure 7: SigS eID enrolment

A user A wishes to generate electronic signatures. The user is using a User Agent (browser) on their computer to enrol. The User Agent sends an enrolment request to the application (back-end at the user's computer), which forwards the request to the SigS (also at the user's computer). The SigS sends an authentication request to an eID service (e.g. the IdMS). The eID service authenticates the user and produces an assertion is then sent to the SigS. The assertion contains identification data (i.e. the minimum dataset). The SigS uses the assertion to send a certification request to a Certification Authority, containing the signature for validation, the CRInfo and an algorithm. The Certification Authority validates the signature and CRInfo and produces a certificate that is then sent to the SigS. The certificate is stored in one of two places: either a hardware security module attached to the SigS or a software-based key store attached to the SigS. The certificate might authenticate a signature for the user, or it might authenticate a signature for a specific application, in which case the user is considered to be the administrator of the application.

Thereby, in eID-based enrolment, processing of personal data happens at the eID service (which is out of scope of this analysis), at the SigS in order to create the key pair and at the CA in order to produce the certificate. Depending on the information stored on the certificate, processing the certificate (e.g. storing in a software-based key store) can in itself be considered as processing of personal data.

[39] Ibid, p. 16.

6.2.4.2 Application-centric signature generation[40]

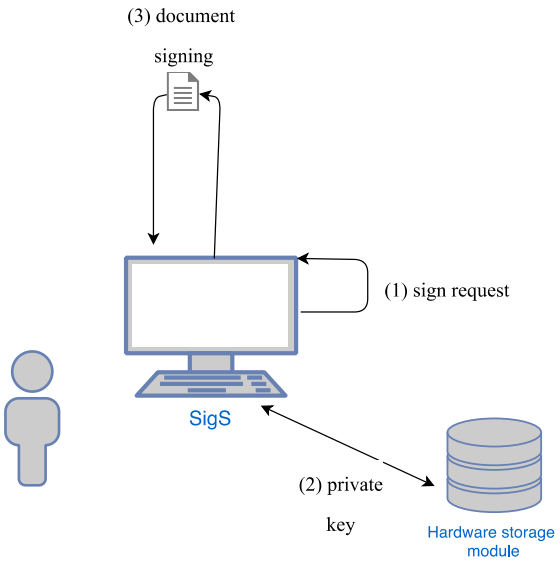


Figure 8: SigS application-centric signature creation

Application-centric signature creation involves the authenticated application and the SigS, but will also involve the storage module attached to the SigS, a smart-card and smart card reader attached to the user's computer or a software key store attached to the SigS, depending on where the user's private key is stored.

In this scenario, the owner of an application system A wishes to produce an electronic signature. The application system sends a sign request to the SigS, containing the data to be signed. The SigS uses the application's private key from the hardware storage module, a software-based key store or a smart card attached to a reader. The SigS generates a signature based on the private key and returns the data in a signature object.

[40] Hühnlein and others, *D3.6 Remote Signing and Sealing, n.* 36, p. 14.

6.2.4.3 User-centric signature generation

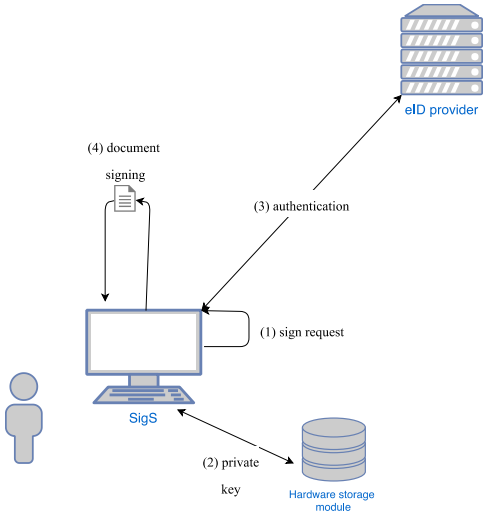


Figure 9: SigS user-centric signature creation

If the user wishes to create a signature using an application-specific key stored at the SigS,[41] the user initiates the request by sending the data to be signed to the application local to their computer. The application sends a sign request to the SigS containing the data to be signed. The SigS sends an authentication request to the eID service of the user (e.g. IdMS or national scheme), which authenticates the user and responds to the SigS with an assertion containing the identity of the user. The SigS generates a signature and sends the signed data as a signature object back to the application.

If the user holds a user-specific key,[42] then the same procedure as above is followed but instead of authenticating at the eID service, the user activates a signature activation protocol that produces an assertion for the user's activation key. Then the SigS receives the assertion from the eID service and unlocks the assertion using the user's private key before generating the signature.

If the user keys are hosted at a remote signing service,[43] then the procedure above is followed but the user activates a signature protocol at the remote signing service through an authentication token. The remote signing service sends the signed response back to the SigS.

Finally, if the user has a smart card signature creation device attached locally to their computer,[44] the SigS performs the same procedure as with the remote eID service, but authentication and identification of the user happens locally (through a card reader).

6.2.5 Data protection roles per use case

The SigS is a software solution that sits at the user's computer. As a result, data processing performed by the SigS is local to the user. The user, in most scenarios, is the data controller (the SigS should not be considered as an entity separate from the user – e.g. a data processor – as it

[41] Hühnlein and others, *D3.6 Remote Signing and Sealing, n.* 36, p.14.
[42] ibid, p.14.
[43] ibid, p. 15.
[44] Ibid, p. 15.

sits at the user's computer and is operated by the user). Therefore, in the use cases of application-centric signature generation and user-centric signature generation where an external eID service or remote signing service is not used, the only actor from a data protection viewpoint is the user who acts as a data controller.

The other use cases, in which there are additional data controllers are described below.

6.2.5.1 eID-based enrolment

In this activity, the user is requesting the SigS to process data in order to register the user so that electronic signatures and seals can be created later on (the purpose is to authenticate the user). The entity determining the means and purposes, therefore, is the user (who is also the data subject providing the personal data). Thereby, **the user is the data controller**. Whether the enrolment is for an application certificate or for a user certificate, the personal data of the user have to be processed to produce the certificate. In the case of an application certificate, the user appears as the administrator of the application system (the natural person responsible for the legal person).[45] In any case, the received certificate is stored by the SigS (a form of processing). The storage location (hardware module, software key store or smart card), as well as the storage duration is chosen by the user.

During the enrolment, two additional entities are involved: an eID service and a Certification Authority. The eID service performs data processing in order to authenticate and identify the user. It makes sense to consider **the eID service as a data controller**.

The Certification Authority, on the other hand, performs processing in order to provide an electronic certificate to the SigS. Assuming they are two distinct services, the Certification Authority **should be considered as a data controller** along with the SigS.

6.2.5.2 Signature generation

The purpose of this flow is to generate a signature on behalf of the user. Where the signature generation is based on a local smart card, data processing happens only by the user in their capacity as the data controller. In this case, because the eID service is the smart card reader attached to the user's computer, and no data transfer takes place with external entities, there are no other actors involved.

However, where signature generation is based on communication to an external eID service, either to authenticate a user with an application-specific key or to create a signature through a signature activation protocol, the external eID service performs processing to produce an attestation for the SigS. Here what was already explained in 6.2.5.1 applies *mutatis mutandis*. **The eID service is operating in its capacity as a data controller**.

Finally, where the user wishes to create a signature through keys hosted at a remote signing service, **the user is responsible for the purposes and means of the creation of an electronic signature and, therefore, the data controller**, and **the remote signing service acts as a data processor** on behalf of the user. [46]

[45] See eIDAS Art. 3(3): "a natural person representing a legal person".
[46] See also eIDAS Rec. 52: "where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, […] remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products,

6.2.6 Data protection by design in the SigS

The purpose of the SigS is to create electronic signature and seals. As such the SigS will be processing two main categories of data: authentication credentials issued to the user and personal data used in the certificates. The data contained in the certificates shall contain "*at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;*"[47] however additional data may be present to the discretion of the issuing qualified trust service provider.[48]

According to eIDAS Article 24, qualified certificates need prior verification of the identity of the natural person who is requesting the certificates. Where the eIDAS infrastructure is used (i.e. where cross-border identification is performed), this amounts to the minimum dataset of a national scheme that satisfies a level of assurance 'Substantial' or 'High'.[49] In other cases though, it requires either a physical presence or an electronic identification with criteria that are set by national laws.[50] Personal data are at the very least processed by eID services, and, depending on the produced attestation, by SigS itself.

The (advanced) electronic signatures should also be considered as a form of personal data, as they are *"capable of identifying the signatory"*.[51] Additionally, since the SigS will have to parse objects (data or documents) to which it affixes electronic signatures, the possibility of processing additional personal data contained within the objects should be acknowledged, especially when such data might be of a sensitive nature in the sense of GDPR Article 9.

At rest data are positioned in a local storage in the user's machine, protected against unauthorised access or unwanted modification by a hardware or software secure key store. Access control is in place, which requires prior authentication of the user.

Because data are stored locally, in application-centric signature generation there is no transmission of data outside of the user's computer. Where external services are used, **confidentiality** of in transit data is secured through the encryption of the channels between the applications and the SigS,[52] and logging ensures the traceability of events.[53] Thereby, risks of unauthorised access to personal data that could lead to the disclosure of either the e-signature or the electronic document the signatures are affixed to are minimised.

The **integrity** of the data is checked against the relevant Certification Authority. Further unwanted modification is blocked through the implementation of access control. Therefore, the controls in place protect against risks of unwanted modification of the e-signatures or the electronic documents that could render the signatures or documents void or lead to electronic documents affixed with wrong or fake e-signatures.

Because of the design of the SigS as a stand-alone product in the control of the user, the personal data used by the SigS are always in the control and the domain of the user. Consequently, their **availability** is protected, minimising risks of disappearance of personal data that could lead to a denial of service or an inability of the user to exercise their rights.

---

including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory."

[47] eIDAS ANNEX I(c).
[48] eIDAS Art. 28(3).
[49] eIDAS Art. 24(1)(b).
[50] eIDAS Art. 24(1).
[51] eIDAS Art. 26(b).
[52] Hühnlein and others, *D3.6 Remote Signing and Sealing, n.* 36, p. 11.
[53] Ibid, p. 12.

Data minimisation is provided for through the support of different authentication protocols (i.e. eID-based enrolment through local eID-card reader) and through the use of hash values when performing electronic signing (pseudonymisation).

In regard to **unlinkability**, the nature of the service implies that a degree of linkability between an electronic signature, the document it is affixed to and the natural person it represents is necessary. However, the SigS ensures that linkability between different electronic documents that have been signed by the same person is not possible, through the use of hashed values to perform the signing (pseudonymisation). The **transparency** of the SigS is ensured through the information prompts that are presented to the user throughout the process of signing. Additionally, the user remains in sole control of the SigS at all times. Finally, the design of the SigS as a service at the user's computer also insures the **intervenability** goal is met: the user is in control of their personal data, their uses and their correctness, as well as the storage periods and erasure.

As a consequence, we obtain the following assessment as regards illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data (*see* the Appendix in section **Fehler! Verweisquelle konnte nicht gefunden werden.** for the complete risk matrix):

Feared event	*Levels of severity/likelihood*	*Control measure*	*Residual risk*
Illegitimate access to personal data (confidentiality)	Significant	Disk encryption; local storage; TLS;	Low
Unwanted modification of personal data (accuracy and integrity)	Significant	Access control; validity checks (e-certificates)	Low
Disappearance of personal data (availability)	Significant	Hardware/software storage modules	Low

Table 5: Controls and residual risks in the SigS

To create and use electronic signatures and seals, the SigS processes authentication data and personal data contained in electronic certificates, but this processing is adequate and directly relevant to the purpose of the SigS.

Additionally, no limitations are imposed on the data subjects, who retain control of the SigS and, therefore, can fully exercise their rights at any given time.

As a result, it can be claimed that processing in the SigS satisfies the **necessity** and **proportionality** principles.

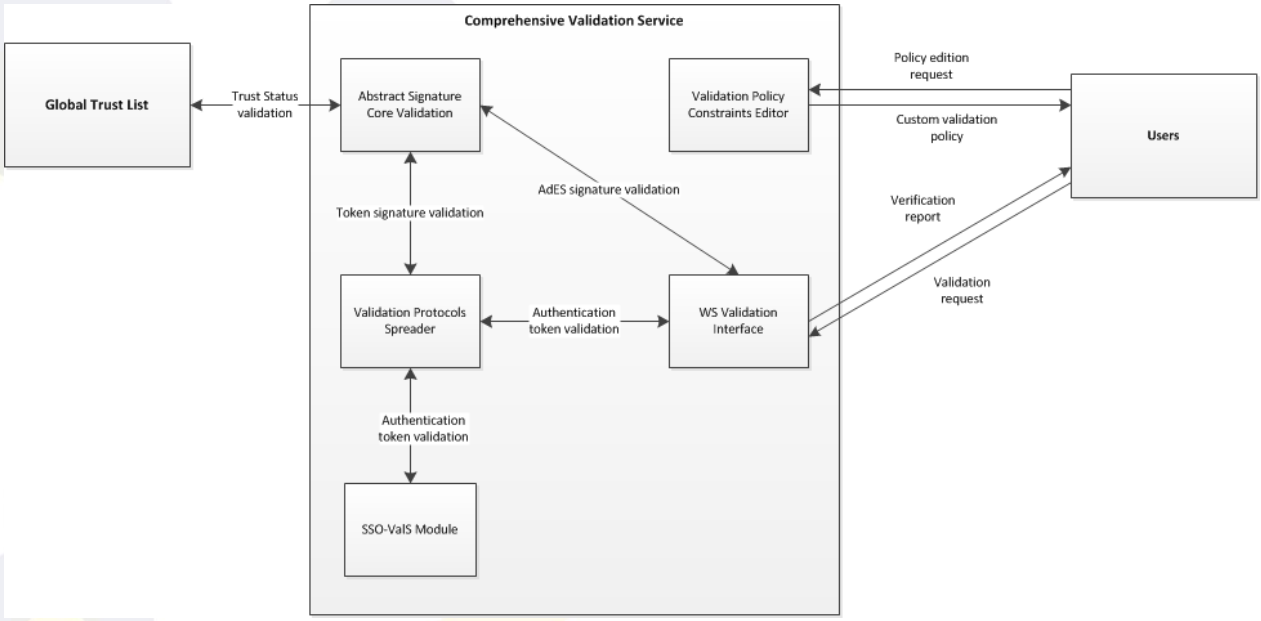
6.3 Comprehensive Validation Service (ValS)

The ValS is designed to satisfy the validation requirements of eIDAS, and in particular with a goal "*to make qualified electronic signature validation easy and convenient for all parties at Union level*".[54] In addition to the validation of various types of electronic signatures and seals, the ValS will be able to create, edit and validate related validation policies, as well as validate authentication tokens. The ValS is designed as a web-service; it will also be provided in the form of an open-source library for integration into existing services.

6.3.1 Stakeholders

The main stakeholders of the ValS are the Trust Service Providers who will use the service in order to provide validation services and the end-users (EU and non-EU citizens) who will be able to request validation of electronic signatures and seals. Aside from citizens, relying parties (other service providers) might also be end-users, where the validation of signatures and seals is needed but the service in question does not want or cannot validate the signature or seal on their own.[55] From a data protection viewpoint, an additional stakeholder is the group of administrators, although their role will in large coincide with the role of the Trust Service Provider operating an instance of the ValS. Finally, the party operating the Global Trust List will also be a stakeholder, where the Global Trust List is used to validate qualified electronic signatures. In addition, service providers (i.e. other than the Trust Service Providers operating the ValS) can use the ValS for verification of authentication tokens. To this end, Identity Providers will also be participating entities.

6.3.2 Data flows



[54] eIDAS Rec. 57.
[55] eIDAS Rec. 57: "relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves".

Figure 10: ValS diagram

From the high-level diagram above, we can see there are three external data flows possible: A validation request made by an end-user to the ValS resulting in a validation report, a validation policy edition made by the end-user resulting in a custom validation policy and a status validation of a Trust Service Provider made by the ValS to the Global Trust List. In place of the Global Trust List, there is the possibility to use the EU Trusted Lists published by the EU Commission. In this case, the data flow will be to the EU List of Lists instead of the Global Trust List.

Additionally, there are several data flows performed within the ValS in between its sub-modules. These will be detailed further in the use cases presented below.

6.3.3 Processing purposes and legal bases

The general processing purpose of the ValS is to validate electronic signatures and seals and authentication tokens. However, sub-purposes exist according to use case (e.g. to create a custom validation policy). These will be explained in the use cases below.

Assessment of the appropriate legal base will at large depend on the Trust Service Provider integrating the ValS into their system. However, as a preliminary remark, possible appropriate legal bases might be of performance of a task carried out in the public interest,[56] performance of a contract,[57] consent[58] and a legal obligation.[59] Given that the scope of electronic signatures validation is to "*ensure legal certainty as regards the validity of the signature*",[60] it seems possible that the legal basis for this type of processing is the enactment of eIDAS, an EU legal instrument, and therefore the basis of the legal obligation of GDPR Article 6(1)(c) will apply.

[56] GDPR Art. 6(1)(e).
[57] GDPR Art. 6(1)(b).
[58] GDPR Art. 6(1)(a).
[59] GDPR Art. 6(1)(c).
[60] eIDAS Rec. 57.

6.3.4 Personal data processing use cases

6.3.4.1 Signature validation

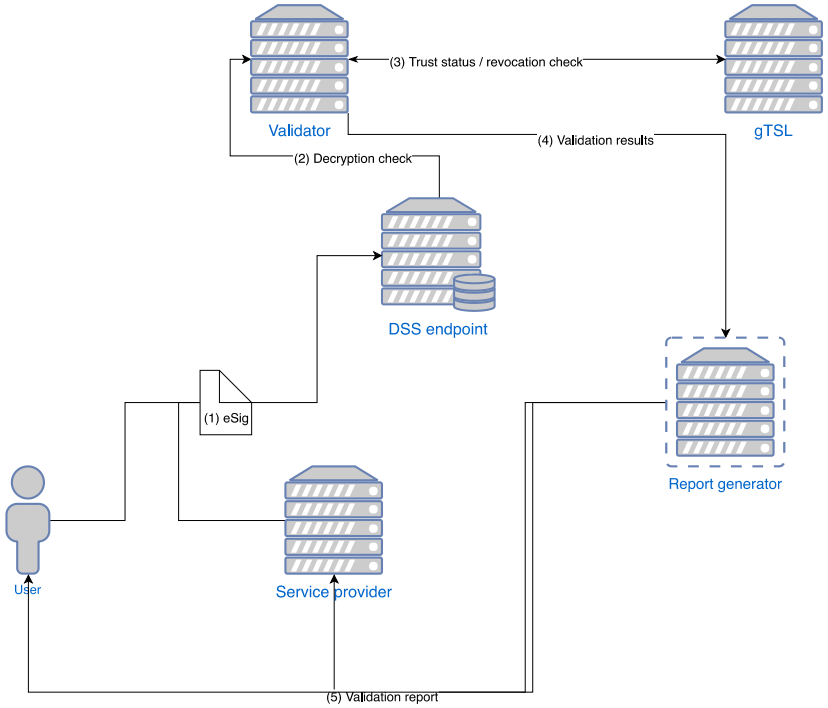


Figure 11: Signature validation in ValS

This use case is similar for all types of electronic signatures supported. The purpose here is to check the validity of an electronic signature, seal or certificate. The entities that initiate a validation request can be either a citizen or a service provider. The request (along with the artefact whose validation is requested) is received by the DSS Endpoint of the ValS and the format is checked to determine if it is supported. The artefact is then sent to the appropriate validator component (CADES/PADES/XADES/ASIC). The validator then checks that the signature's encrypted value (encrypted by the related certificate's private key) can be decrypted by the certificate's public key. For certificates, it also ensures that the related certificates were valid at the claimed signature creation time. The validator contacts the Global Trust List to check the status information of the Certificate Authorities and retrieve revocation information from Certificate Revocation Lists (maintained outside of the gTSL). If, instead of the Global Trust List, the EU List of Lists are used, the published Member States lists would have been downloaded locally, so trust status will be checked locally. The results are sent to the report generator sub-module, which composes a report for the validation requested. The report is sent to the DSS Endpoint, which transmits it to the requestor.

The users can submit requests with embedded signature objects (signatures or timestamps). Additionally, the user can supply optional inputs to help validate the signature. The optional input can contain the identity that the user would like to validate the signature against (ClaimedIdentity).

The signature object should be considered as personal data, since an advanced and a qualified electronic signature are "*capable of identifying the signatory*".[61] The ClaimedIdentity input might also be considered as personal data to the extent that it contains information that assist in making the data subject identified or identifiable. The validation result that is returned to the user does not contain personal data, unless the optional input of ClaimedIdentity was used in which case it is contained within the validation report.

6.3.4.2 Token, certificate and evidence record validation

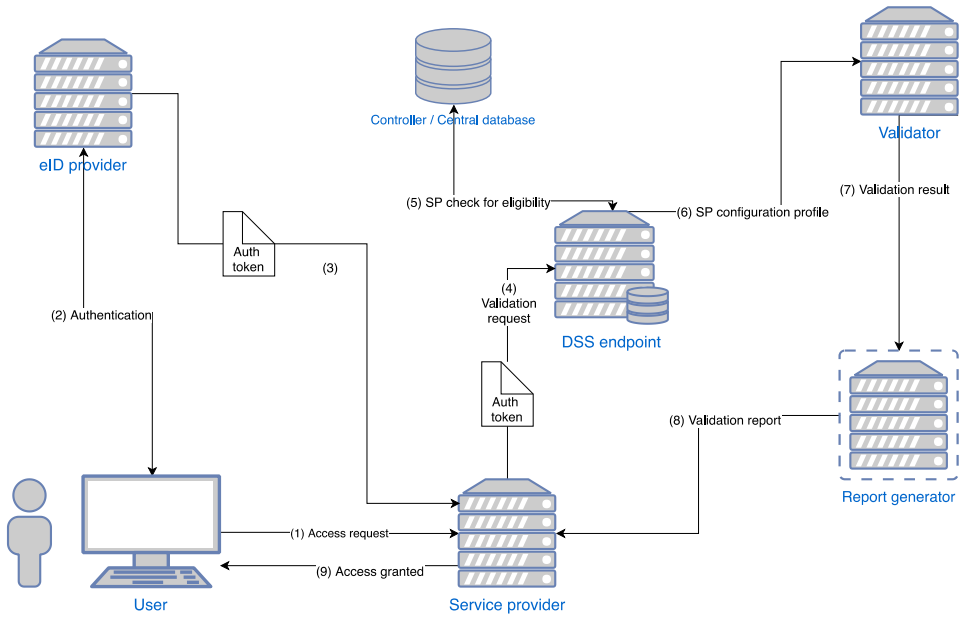


Figure 12: Token validation in the ValS

In this use case, the purpose is to verify that a specified authentication token (SAML, OAuth or OpenID Connect) is valid and subsequently used for single sign on to third party services. The users of this use case, therefore, are service providers wishing to authenticate natural persons. There are several resulting sub-processes that involve additional actors: in token verification, the ValS needs to communicate with an Identity Provider who will perform the identification of the user and produce an authentication token; at the same time, the ValS supports configuration of verification templates, defining the rules that the verification of the tokens of each Identity Provider will happen, which will involve administrators from the Identity Providers; finally, the operator of the ValS will have administrators that will manage the Identity Provider list, configure the web service and produce logs. Apart from token validation, no other process involves personal data.

[61] eIDAS Art. 26(b).

The configuration processes (managing the Identity Provider list, configuring the web service and logs) involve the creation and storage of authentication data, however since that data relate to legal entities (the service and Identity providers), they are not personal data.

In typical single sign on scenarios, the data subject (natural person) will ask to access a service. The service provider will redirect the data subject to their Identity Provider. The Identity Provider will perform an authentication and produce an authentication token, which will be sent to the service provider. The service provider uses that token, which it validates against the Identity Provider, to grant access of its service to the user. Although this whole procedure involves processing of personal data, most of it is out of scope for our purposes since it is unrelated to the ValS. The ValS aims to substitute only the token validation part of the process and, thus, only the processing of personal data involved for this process will be considered below.

Token validation begins with a sender (service provider) making a request to the operator of the ValS, including the authentication token. A Controller module in the ValS then checks against its list of providers to determine whether the sender is authorised to make such a request, by authenticating the sender against credentials stored in a Central Database. If the sender authenticates successfully, then the controller will load the relevant configuration profiles from the Central Database. The verification request is then sent along with the profile to a Verification module. The verification is executed and the result is returned to the Controller. The Controller generates a report and sends it to the sender.

The report may contain, aside from the success or failure of the verification, optional outputs. In the optional outputs, details about the followed procedure are explained, but also an attribute *authenticatedUser* which contains the information regarding the authenticated user (unique identifier and optionally email address, phone, age or gender).

6.3.4.3 Policy validation, creation and export

In this use case the purpose is to define, enquire about or validate a validation policy. This allows for the expansion of the ValS to support new or not-yet known formats of electronic signatures and certificates. The end-user (citizen or administrator) send a request to validate or edit a policy. If the request is to create a new policy, the policy validator loads a policy template and presents it to the user for editing. The user edits the policy in browser and submits the result. The resulting document is checked by the policy validator against policy rules. The validated policy is returned to the user.

In case of policy validation, the policy validator loads the specified policy template. Then the same procedure as above is followed, with the end result being returned to the user.

The policy use cases target rules on validation processes and, as such, do not contain personal data. They are, therefore, out of scope for the purposes of this analysis.

6.3.4.4 System management

The system management includes processes meant for the upkeep of the system (managing of administrator accounts, policy templates, processing rules etc.). As such, processing of personal data for these use cases is related only to the data of the persons that act as system administrators (login credentials, contact details etc.). As these will be governed under the related policies that the operator of the ValS have in place for their employees, they will not be explored here.

6.3.5 Data protection roles per use case

6.3.5.1 Signature validation

As mentioned above, this process is initiated by the end user, which can be either a natural person or a service provider. In other words, in this use case, the end user is the entity that controls the purposes of the processing (the validation of the electronic signature or timestamp). **The end user is, therefore, a data controller**.

On the other hand, the ValS, operated by a provider, performs processing on behalf of the end user. Even though the means of the processing (what and how data will be processed) is selected by the ValS, it is dependent upon the format of the received signature object and mandated by international standards (e.g. CADES). Therefore, the means of the processing could also be said to be controlled by the end-user, who is supplying the signature object. **The provider operating the ValS, thus, should be considered a data processor** that perform processing on behalf of the end-user.

6.3.5.2 Token validation

In token validation, the process is initiated by the service provider requesting the authentication. Even though the natural person selects the applicable Identity Provider to perform the authentication, it is doubtful whether the person has actual control over this selection, especially in cases where the Identity Provider is the official notified scheme of their country of origin. Therefore, the purposes and means of the processing in token validation are controlled by the service provider and the Identity Provider is performing processing on behalf of the service provider. **The service provider should be seen as the data controller** in this instance, with **the Identity Provider being a data processor**. **The natural person, on the other hand, is the data subject**.

The operator of the ValS is performing processing for token validation according to the instructions of the service provider and the Identity Provider. **The operator of the ValS**, in other words, **is a data processor** on behalf of the service and Identity providers.

However, the operator of the ValS might hold a data controller role in regard to data processing performed for the management of the authenticated providers. If any personal data are held regarding the services that can authenticate and access token validation (e.g. the contact details of the person in charge of the respective service provider), **the operator of the ValS will be considered a data controller for any processing towards the management of third-party service providers**.

6.3.5.3 System management

For any processing relating to the system administrators, **the operator of the ValS is a data controller**, in the same capacity that the operator is a controller of the data of all other employees.

6.3.6 Data protection by design in the ValS

The ValS processes two main types of personal data: Personal data relating to electronic signatures and timestamps and personal data relating to authentication tokens.

In token verification, one of the supported methods of authentication is *pop*, in which no credentials are sent through the network. Therefore, the ValS is designed to provide a way to minimise the processing of personal data needed to verify an authentication token.

The main risks associated with the operation of the ValS arise in the event of unauthorised access to the personal data. Unauthorised access can result in the disclosure of either the electronic signatures and seals or the electronic documents they accompany. In the scenario where the ValS is used for token authentication in single sign-on configurations, the impact of the risks might even result in impersonation of a data subject (identity theft). Core controls have been implemented in the ValS to mitigate such risks.

Data minimisation is further advanced by the ValS' ability to validate electronic signatures and timestamps only by validating the signature object's hash value. Consequently, unless extraction of the signature object is impossible, no data contained in the embedding document will be transmitted or processed.

Integrity of the data is ensured through the implementation of the SSO-cache module against replay attacks.[62] However, we should note that the personal data processed by the ValS, namely for the validation of authentication data, are not stored by the ValS. The central storage in the ValS is intended for information on the registered service providers and their policies. Consequently, there are no significant risks for the **integrity** and **availability** of personal data, i.e. the unwanted modification or deletion of personal data.

Finally, the **confidentiality** of data in transit is secured through TLS encryption[63] and the ValS performs an 'encrypt-then-sign' function to secure confidentiality and integrity prior to transmission.[64] At rest, access control is implemented in the ValS through the mutual authentication between the parties,[65] the support of the OpenID protocol and access rights for the group of administrators.

In terms of **unlinkability**, the ValS might be said to enhance the unlinkability afforded in scenarios of electronic authentication by operating as a broker in between a service provider and an identity provider. Since the ValS is performing the token authentication, the origin of the request (the identity of the service provider) is hidden from the identity provider and, equally, the identity of the identity provider is not disclosed to the service provider. Evidently, this is the case when the ValS is operated by an entity other than the identity or the service providers. We should acknowledge, however, that in this scenario the ValS might be able to profile the activity of the user, since the ValS will know both the origin and the target of the request. This risk should be considered as of low probability, though, since the ValS does not store logs of activity and data in transit are encrypted.

The goals of **transparency** and **intervenability** will depend on the policies and practices of the relying parties (the identity and service providers), since the ValS does not store personal data; information about the processing are given to the users when they are prompted to select

[62] Vincent Bouckaert and others, *D3.3 - Comprehensive Validation Service* (final v 1,00, FutureTrust project, 30 May 2017), p. 49.
[63] Ibid, p. 13.
[64] The 'Encrypt-then-sign' functionality allows the ValS to validate messages that were signed after encryption. This way the ValS is able to validate them without being able to read the contents of the message. This functionality is introduced first to JSON and XML formats, with implementation in other formats, like PDF, being currently examined.
[65] Hühnlein and others, *D3.6 Remote Signing and Sealing, n.* 36, p. 24.

functionality (validation of signatures, of seals or of authentication tokens), but data subject rights should be exercised at the level of the identity and service providers.

As a consequence, in regard to illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data, we obtain the following assessment (*see* the Appendix in section **Fehler! Verweisquelle konnte nicht gefunden werden.** for the complete risk matrix):

Feared event	*Levels of severity/likelihood*	*Control measure*	*Residual risk*
Illegitimate access to personal data (confidentiality)	Significant	TLS; 'encrypt-then-sign' access control	Low
Unwanted modification of personal data (accuracy and integrity)	N/A	SSO cache; 'encrypt-then-sign'	Low
Disappearance of personal data (availability)	N/A	Stateless operation	Low

Table 6: Controls and residual risks in the ValS

The ValS satisfies the **necessity** principle since it only processes data (electronic signatures, seals and timestamps and authentication data) when strictly necessary to perform validation. Where the purpose permits, no personal data are processed (as is the case with authentication data during the *pop* method).

In addition, the ValS uses proportionate means to satisfy the aim: validation is performed on an extracted object (electronic signature, seal or authentication token) rather than processing the container of the object (e.g. the electronic document). Thereby, the ValS satisfies the **proportionality** principle.

6.4 Global Trust Service Status List (gTSL)

The gTSL is designed to assist in managing and providing information related to Trust Service Providers and the related trust services, extending the current Trust Service List model to include non-EU trust service providers.

The gTSL is designed as a stand-alone service that allows Trust Service Providers to advertise their trust services and citizen to query them. It extends the current Trust Service List devised by eIDAS in that it allows for decentralised storage of the lists of trust services, it records changes in trust services' status, while offloading the updating of the available trust services from the national points of contact to the individual Trust Service Providers. Instances of the gTSL can be hosted with a Trust Service Provider or integrated into the national lists systems of the Member States.

Because of the design and the nature of the service, the gTSL does not rely heavily on processing of personal data. Most of the data processed by the service are related to information concerning legal persons (the Trust Service Providers) and their products (the trust services). As a result, the analysis that will follow will only focus on the individual processes in the system that process some form of personal data.

6.4.1 Stakeholders

The actors involved in the gTSL belong to three groups: Member States administration, Trust Service Providers and citizens.

EU Member States are responsible for curating and releasing to the EU Commission a national list of the qualified Trust Service Providers and the trust services they provide and, optionally, non-qualified trust services.[66] The gTSL allows the administrators of such lists to offload that responsibility to the gTSL.

Trust Service Providers are meant to notify their supervisory body about their qualified trust services, after which the supervisory body publishes that status in the national lists.[67] The gTSL will allow them to monitor and update their qualified status directly, with the changes reflected in the national and global lists.

Administrator of trust lists from non-EU states will be able to use the gTSL to advertise their (equivalent) trust services in the trust lists maintained by the gTSL.

Citizens of EU and non-EU countries will be able to query the gTSL in order to discover trust services that fit their needs.

Finally, administrators of the gTSL are responsible for enrolling new authorised users that can manage trust lists and are in charge of the maintenance of the gTSL.

[66] eIDAS Art. 22(1).
[67] eIDAS Art. 21.

6.4.2 Data flows

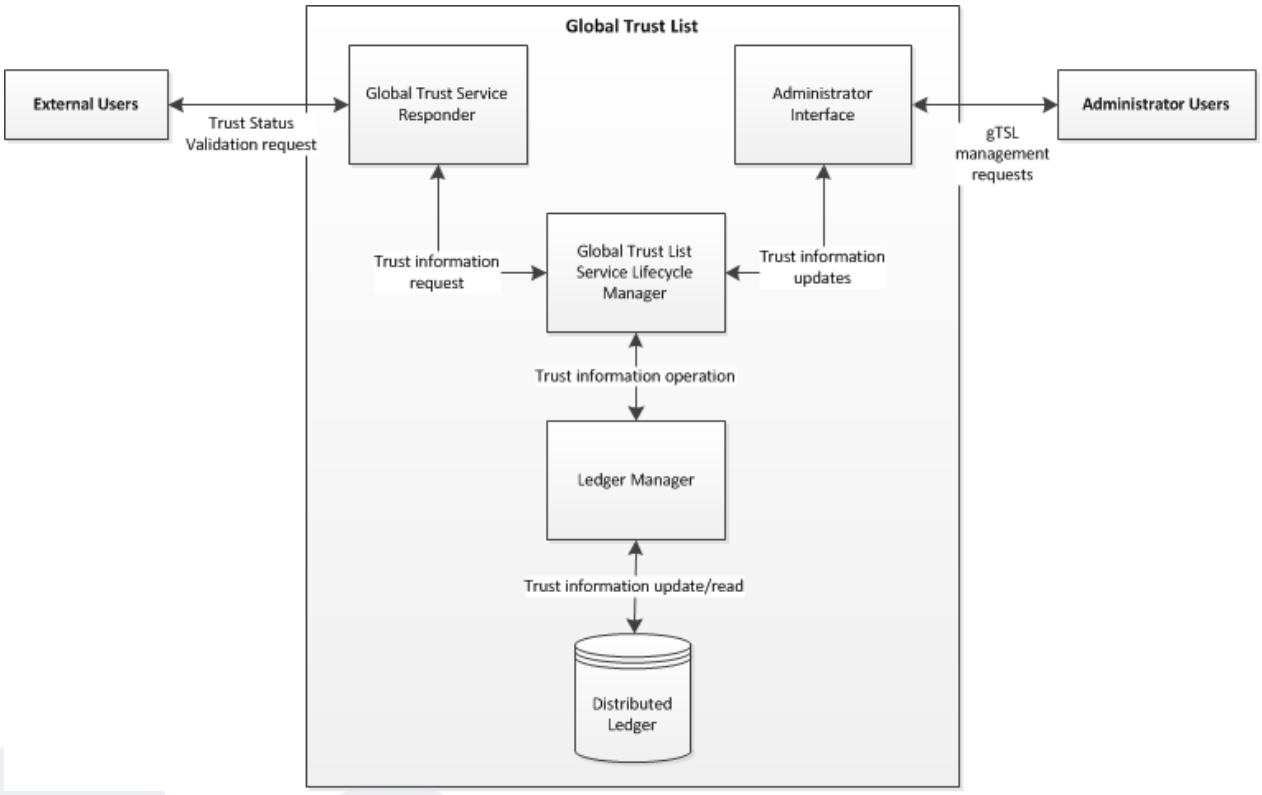


Figure 13: gTSL data flow diagram

The gTSL comprises several sub-components: an Administrator Interface to allow authorised users to add, update and delete trust lists and trust service providers; a Service Lifecycle Manager that handles the hierarchy of recorded trust services and allows updating their status through a Ledger Manager that communicates with the Lifecycle Manager and Distributed Ledgers that hold the information on trust services in a block chain. Finally, a Global Trust Service Responder that allows external users (citizens) to query the information that the gTSL holds.

The basic data flows allow administrators of trust lists and of Trust Service Providers to manage the status of available trust services and citizens to gather either whole lists of trust services for a particular location or individual trust services available to them. However, since this process concerns information about legal entities and services, it is out of context for this analysis.

The relevant data flows for data protection are to do with the authentication of users with administrative rights, a notification function provided to citizens for updates on trust services and, exceptionally, the process of signing for a trust service list, when that signature is linked to a natural instead of a legal person.

6.4.3 Processing purposes and legal bases

The main purpose of the gTSL is to provide information on Trust Service Providers and their trust services. However, this purpose is unrelated to the (little) data processing that is performed in the system. Personal data processing in the gTSL happens only for one of three purposes: to

authenticate users to the system so that they can perform administrative tasks; to notify them of changes to trust services after they have expressed their interest in such notifications; and, to allow them to publish trust service lists, when the electronic signature used is linked to a natural person.

From these three purposes, the last one is mandated by law (eIDAS Article 22(2)). As such, it is likely that the appropriate legal basis will be found in the necessity to comply with a legal obligation.[68]

Administration of the trust service in the gTSL will likely happen after a contract, either of the Trust Service Provider with the operator of the gTSL, or the Trust Service Provider with its employees if the gTSL is integrated in the Trust Service Provider's system. In this case, the processing will be necessary for the performance of the contract[69] or the legitimate interests of the data controller.[70] This does not preclude the use of the legal obligation basis, when the operator is the national body responsible for the national trust list.

As for the notification functionality, processing is likely to be based on consent since it is an optional function, offering added value that is however unrelated to the purpose of the gTSL (to hold lists of Trust Services), that requires the data subject's opt in.

6.4.4 Personal data processing use cases

6.4.4.1 Authentication

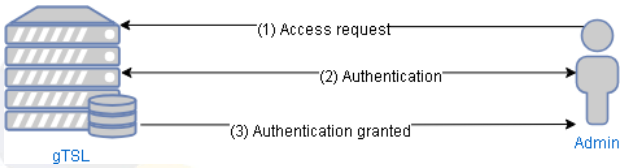


Figure 14: Authentication in the gTSL

Management of the trust services and trust service lists is done by a group of users with administrative roles either on behalf of the Trust Service Provider or the body in charge of the national trust service list. In order to gain access to administrative functions, a user needs to authenticate to the gTSL. Authentication of administrators is handled by Ethereum, the block chain technology that manages the distributed ledgers. The administrators authenticate using their account's private key.

[68] GDPR Art. 6(1)(c).
[69] GDPR Art. 6(1)(b).
[70] GDPR Art. 6(1)(f).

6.4.4.2 Notification

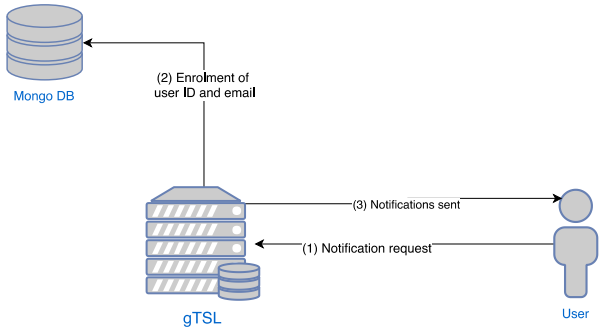


Figure 15: Notification enrolment in the gTSL

In respect to the citizens using the service, querying the gTSL happens without a need for any personal information exchange. However, citizens have the option to subscribe to receive notifications for changes to trust services of interest. In order to subscribe, the user selects a trust service list notification channel and submits that preference. Along with their preference, the user submits their email address where the notifications will be send. The two are stored in a local database, along with a unique id created for this purpose. Whenever a change happens on a trust service list, the system looks through the database and notifies all the email addresses that have subscribed to the channel of that list.

6.4.4.3 Sign or import a trust service list

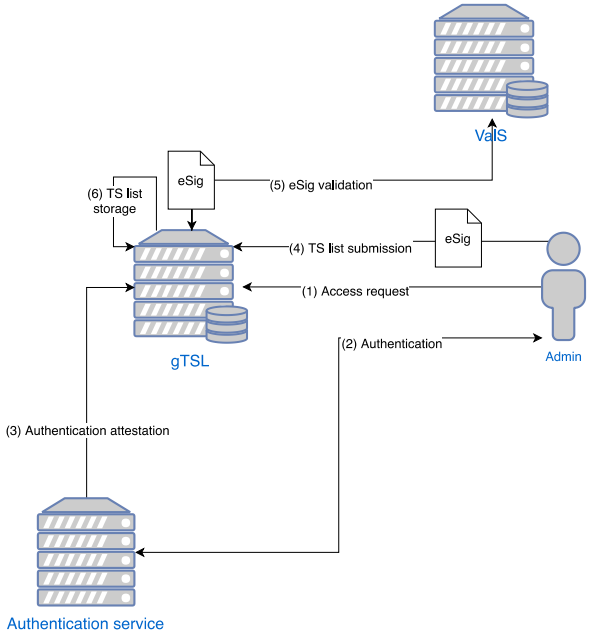


Figure 16: Import of a Trust Service list

In order to publish a trust service list, the system requires that the list is signed in accordance with eIDAS Article 22(2). In order for this, the gTSL requires communication with an external validation service (like the ValS) that will check for the validity of the provided signature. In practice, this means that when an administrator submits a signed list for publication, the gTSL files a request to a validation service with the provided signature and receives a validation report back (the data flow performed for validation is not relevant here). If the validation of the signature succeeds, the gTSL stores the trust service list along with the signature in its ledger. A success message is returned to the administrator upon successful storage.

6.4.5 Data protection roles per use case

6.4.5.1 Authentication

The purpose of personal data processing in this use case is to elevate the rights of certain users so that they are able to manage the status of trust service providers and trust service lists. Information about which accounts are authorised to administrate trust services is saved in the block chain (accessible through the *gtsl-admin* component) in the form of smart contracts. The smart contract contains a list of the block chain (Ethereum) account addresses that are authorised to perform administrative functions.

The users are authorised by using their account's private key. **The gTSL is, therefore, the data controller**.

6.4.5.2 Notification

Users who wish to be notified for changes to trust service lists have the option to subscribe to such notifications. The purpose, therefore, is to provide a notification service to the user. The user initiates the subscription process and submits their email address and their preference as to which services they should be notified about. This information is saved in a local database (MongoDB) in the *gtsl-web* component. Here **the data controller is the gTSL** who provides a service to the user after the user's consent. If an external subscription provider is used to send the notifications, then **the processing that the subscription provider performs is in its capacity as a data processor** on behalf of the gTSL (*SubscriptionProvider* external component).

6.4.5.3 Sign or import a trust service list

Signing is required in order to publish trust services lists. The purpose of the processing, therefore, is to provide the users with the ability to publish trust service lists in conformity with eIDAS. It is important to note that when the lists are signed with an electronic signature belonging to the body responsible for the national lists, no personal data are processed, since electronic signatures of legal entities need only contain "*the name and, where applicable, registration number as stated in the official records*".[71]

It is at the moment unknown whether authorised representatives of such bodies are allowed to use their personal electronic signatures to sign the lists. In this case, the signature will contain personal data since it links and identifies the signatory (the representative). In this case, **the body responsible for the list is the data controller** who determines the purposes (the publishing of the list) and the means (using an electronic signature of a representative). **The gTSL and the external validation service are data processors** on behalf of the data controller who verify that an electronic signature exists and is valid before publication.

6.4.6 Data protection by design in the gTSL

The gTSL processes two categories of personal data: authentication data of users that belong to the administrator group, in order for them to perform administration functions (e.g. to publish a new Trust Service list); and personal data used for the notification functionality of the gTSL, i.e. in order to notify interested users about changes in the Trust Service lists.

As a result, risks to the personal data of data subjects are limited, since only email addresses of the data subjects are kept. Risks of unauthorised access to the stored addresses or unwanted modification or deletion of them will result in the malfunction of the notification component. However, since the sole purpose of the component is to notify the data subjects about changes in trust service lists (which contain no personal data), no further impact upon their freedoms or rights is likely. Additionally, the risk of modifying personal data for administration account in order to gain administrative access to the system will have minimal impact since the administrative functions are dependent on the block chain and, hence, are easily monitored.

The **confidentiality** of the data is secured through the communication between the gTSL and third parties via TLS encryption. Access control is in place to ensure authorised access to functions and data reserved for administrators.

[71] eIDAS ANNEX I(b).

Additionally, the personal data that are held at rest in storage are also encrypted (both in the block-chain and in the Mongo databases), in order to guarantee their **integrity**.

The **availability** of the data can be safeguarded by duplication of the Mongo DB (back up of the database).

Finally, to provide notification functionalities, **data minimisation** is applied through the processing of only the email address of the data subject, which is then associated with a pseudo-random unique identifier.

The data minimisation applied also reinforces **unlinkability**: no further information is held to link the email address (which does not have to be associated to the real identity of the data subject) to the data subject itself. Suitable privacy notices about the processing and storage of data for the notification functionality will affect **transparency** and the data subjects will be able to request the removal or update of the recorded email address (**intervenability**).

Therefore, in terms of illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data, we obtain the following assessment (*see* the Appendix in section **Fehler! Verweisquelle konnte nicht gefunden werden.** for the complete risk matrix):

Feared event	*Levels of severity/likelihood*	*Control measure*	*Residual risk*
Illegitimate access to personal data (confidentiality)	Significant	TLS; disk encryption; access control	Low
Unwanted modification of personal data (accuracy and integrity)	Significant	Disk encryption	Low
Disappearance of personal data (availability)	Significant	Disk encryption	Low

Table 7: Controls and residual risks in the gTSL

The gTSL satisfies the **necessity** and **proportionality** principles because it does not require by default the processing of data outside of the strictly necessary to publish Trust Services statuses. Processing that is not strictly necessary for this purpose (the notification function) is only offered on an opt-in basis.

6.5 Scalable Preservation Service (PresS)

The purpose of the PresS is to ensure the long-term preservation of electronic signatures and seals, extending the trustworthiness of the (qualified) electronic signatures and seals beyond their technological validity period by providing a 'proof of validity' and 'proof of existence'.

The PresS is designed as a service that is meant to be interfaced with a validation service (like the ValS), a time stamping authority and external storage services.

6.5.1 Stakeholders

The parties involved in the PresS are Trust Service Providers who wish to provide a preservation service, or already provide time stamping and/or validation services that are interfacing with the PresS; storage providers, who may provide storage services for the PresS; and finally, transaction service providers (e.g. organisations or governmental bodies), who will be the users of the PresS.

Two additional groups have access to the PresS: administrators and auditors. Administrators work for the entity operating the PresS (the Trust Service Provider). Auditors may work for the Trust Service Provider or may be external entities who wish to verify the PresS' operation according to policy requirements.

6.5.2 Data flows

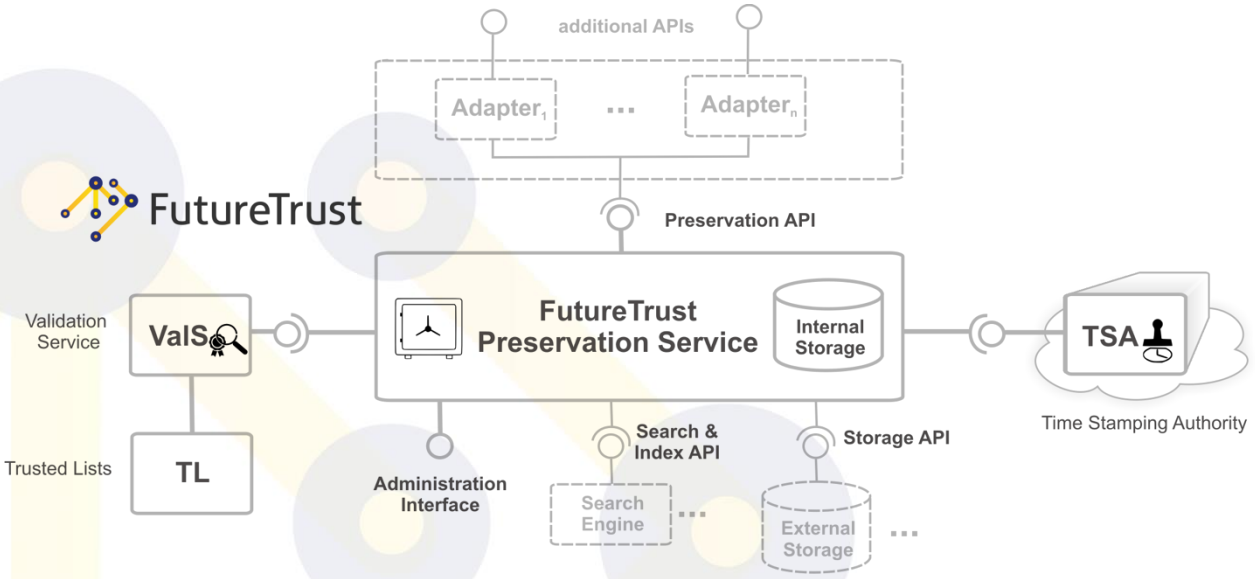


Figure 17: The PresS diagram

Figure 17 provides an abstract overview of the PresS. It should be assumed that the validation and time stamping services depicted here can either be integrated in the same system as the PresS or provided by a different entity. In any case, their data flows will be considered black-boxed for this analysis.

Users (transaction service providers) can deposit, update, retrieve or delete electronic signatures and seals for preservation through the Preservation API. The electronic signatures and seals are

stored in Preservation Object Containers, in internal or external storage (if an external storage provider is used). The functionality is offered through a Preservation Service Interface. The Interface interacts with the Preservation Service Core, which is in charge of parsing the Preservation Object Containers with a validation service and a time stamping service before handing it on to data storage. A Search and Index Adapter is also connected to the Interface, so that Object Containers are searchable.

6.5.3 Processing purposes and legal bases

The overall purpose of the PresS is to provide 'proof of integrity' and 'proof of existence' to trust services, and/or extend the validity of a digital signature or time assertion, by managing Preservation Data Objects. Additional goals include the ability to maintain the confidentiality and availability of the preserved data and demonstrate this by traceability of actions.

PresS' overall purpose derives from an eIDAS Article 34: the provision of "*procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period*". However, long-term preservation of trust services is not an eIDAS requirement strictly speaking; it is rather an additional trust service offered to entities that wish or are required by legislation or policies to preserve electronic documents containing an electronic signature or seal for a period that exceeds the validity of the signature or seal. It is most likely that the legal basis will be the performance of a contract between the user and the PresS.

6.5.4 Personal data processing use cases

6.5.4.1 Deposit/Update/Retrieve/Delete/Search Preservation Object Container

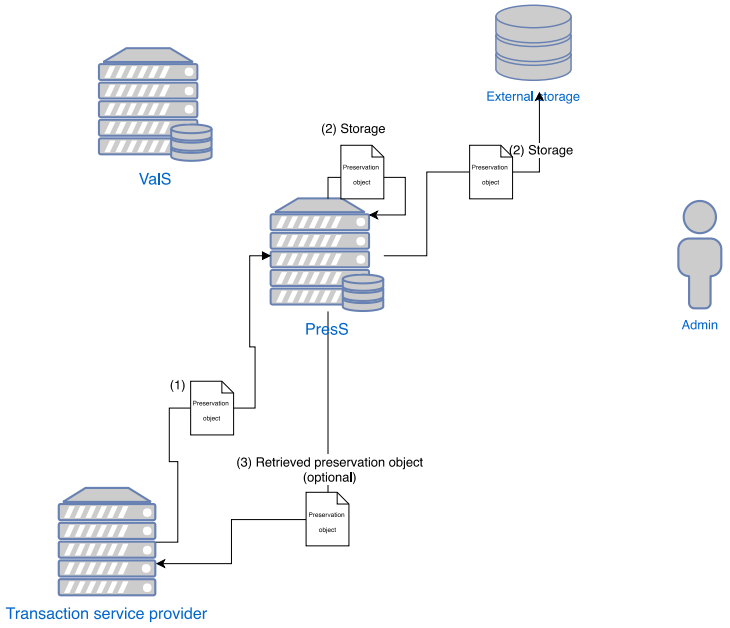


Figure 18: Preservation objects in the PresS

The data flows to deposit, update or retrieve electronic signatures as a Preservation Object Container, to delete an existing Container or to search within the available Containers are pretty similar.

An authenticated user (a transaction service provider) accesses the Preservation Service Interface. To deposit an electronic signature or seal, the Interface sends the signature or seal as a Preservation Data Object to the Preservation Service Core, where the Core affixes a time stamp, generates an ID for the Container and sends the Container to data storage.

Similarly, to update, retrieve or delete a Container, an authenticated user submits the Container's ID, along with any modifications as simplified objects. The Core either updates the Container and sends it back to storage, or sends the Container to the user in the case of retrieval or deletes the Container.

In the case of search, a user can provide a query to the search module which will return a list of IDs of containers that fit the search criteria.

6.5.4.2 Verify Preservation Object Container

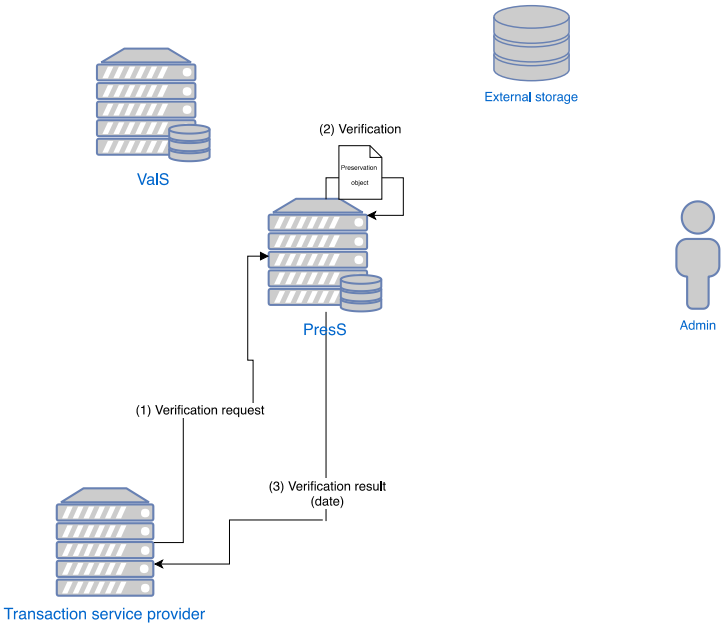


Figure 19: Verification of objects in the PresS

A user can ask for the verification of Container (by Container ID). The verification process verifies the data objects themselves as well as the evidence record and the associated certificates of the Container. The result of the verification returned to the user is a date that indicates the existence of the Container.

6.5.4.3 Augment electronic signature

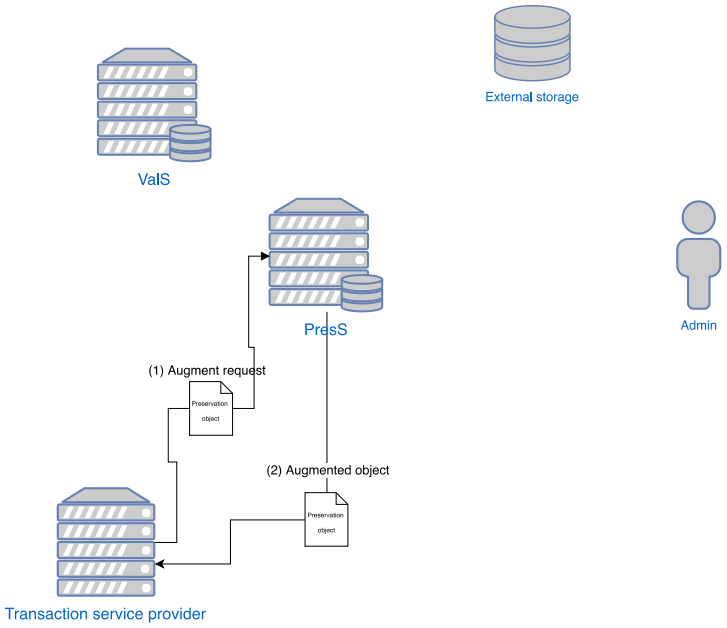


Figure 20: eSignature augmentation in the PresS

This process does not store the electronic signature at the PresS. It can be used to create a long-term signature based on an electronic signature by affixing archive timestamps. The user provides the electronic signature, the Interface sends it to the Core, the Core communicates with the Time Stamp Authority and creates a long signature that contains the original signature and a timestamp. The long signature is returned to the user.

6.5.4.4 Retrieve proof

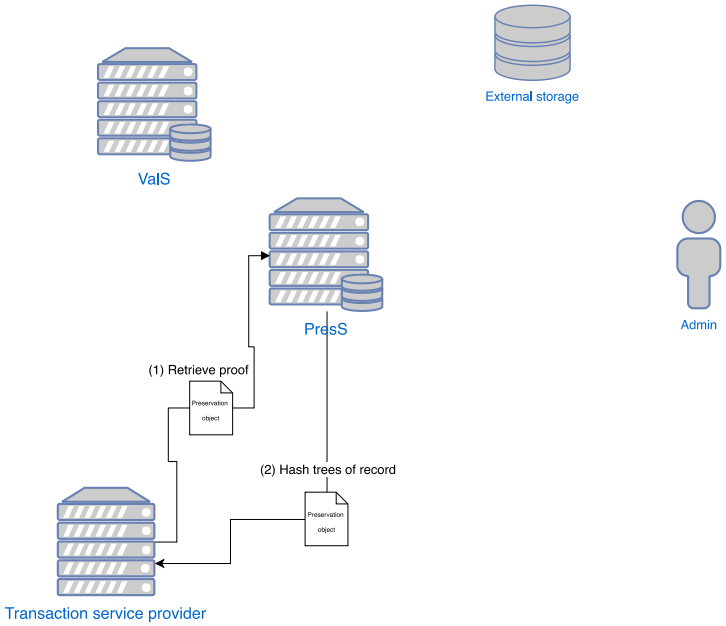


Figure 21: Proof retrieval in the PresS

An authorised user can retrieve an evidence record for a Container. The evidence record contains the hash trees of all archive time stamps associated with the Container.

6.5.4.5 Administration

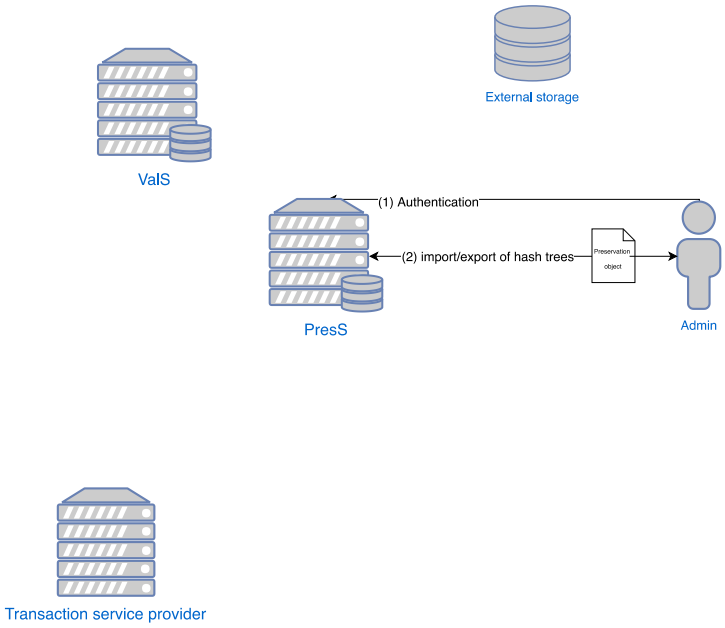


Figure 22: Administrative functions in the PresS

Administrators of the system have management rights. Apart from managing the preservation policies for each user (which should not include personal data processing), they can import and export the full set of internal data including hash trees (the unique hashes associated with Containers). In this case, depending on the information accompanying the hashes, the hashes might be considered pseudonymised data in the context of GDPR Article 4(5). Finally, the administrators have the capability to initiate a renewal of the timestamps or hash-trees associated with the Containers (which should not in principle be considered as personal data processing).

6.5.4.6 Auditing

Auditors are able to retrieve auditable logs which prove the compliance of the PresS with respect to specific policy requirements. However, the logs should not in principle contain personal data.

6.5.5 Data protection roles per use case

6.5.5.1 Deposit/Update/Retrieve/Delete/Search Preservation Object Container

The purpose of processing in this use case is to allow the preservation of electronic signatures and seals by the interested consumers (transaction service providers) of the system.

Two sets of personal data are processed for this operation: first, personal data needed for authentication of the consumer of the service (the user); second, personal data relating to the electronic signature or seal being preserved.

For the first set of data, the operator of **the PresS (the Trust Service Provider) is the data controller**, since they are responsible for determining the data required to create an account for the user and when that data will be used (i.e. during authentication, during marketing etc.). The consumer (the transaction service provider) is the data subject.

For the second set of data, the consumer (the transaction service provider) is the entity that decides which data (which electronic signature, for example) will be used and for which purpose (e.g. to augment it or to archive it). Hence, **the consumer is the data controller**. The operator of the PresS processes data on behalf of the consumer, i.e. **the operator of the PresS is the data processor**. Any external **time stamping, validation or storage services are data processors** as well.

6.5.5.2 Verify Preservation Object Container

Mutatis mutandis, the same must apply for the verification of a Container. Although the verification result is only a date, the verification process requires the validation of all the objects of a Container, i.e. requires processing of the personal data contained within. Again, **the consumer acts as a data controller, with the operator of the PresS acting as a data processor**.

6.5.5.3 Augment electronic signature

Mutatis mutandis what was described in 6.5.5.1 and 6.5.5.2 above.

6.5.5.4 Retrieve proof

The operator of the PresS acts again as a data processor on behalf of **the data controller who is the consumer**. Whether the hashes that are processed to produce the evidence record will be considered as pseudonymised data or not is of little importance, since processing of pseudonymised personal data is still considered processing of personal data.

6.5.5.5 Administration

The last use case that processes personal data is part of the administration functionality, and in particular the ability of the administrators to import or export the full set of internal data. Characterisation of this process in terms of data protection roles is hard, because the exact circumstances and purposes where this process might be used is not known. If the process is used internally by the operator of the PresS to serve a purpose the operator has, then **the operator of the PresS should be considered as the data controller**.

6.5.6 Data protection by design in the PresS

The PresS processes three categories of personal data: personal data required for the authentication of the end-users (the users that consume preservation services); personal data for the administrators of the PresS; and personal data relating to the preservation of electronic signatures and seals.

The **confidentiality** of the processed data is ensured through cryptography. Additionally, support in the PresS of ‘time-lock-encryption’ has been proposed, but its feasibility is currently being

examined.[72] The PresS supports access control, allowing access to administrative functions only to authorised users.

The **integrity** of the preserved data is protected through the establishment of 'preservation policies' (a set of technical rules the PresS follows according to the preserved object).

The **availability** of the data is maintained through the ability to duplicate or supplement the internal storage via external storage locations.

The PresS applies **data minimisation** through the use of pseudonymisation (hashed values) on the preserved data objects and the ability to supply long-term preservation without storage of the data object.[73] The data minimisation is also effecting **unlinkability**, since the pseudonymised data cannot be linked to the originating data without additional information.

The **intervenability** rights of the data subjects, as well as their right to **transparency**, should be sought against the users of the PresS, namely the transaction service providers; however, since the PresS supports preservation without storage of the data, rights to object to processing, modification or erasure are not applicable.

Consequently, for illegitimate access to personal data, unwanted modification of personal data and disappearance of personal data, we obtain the following assessment (*see* the Appendix in section **Fehler! Verweisquelle konnte nicht gefunden werden.** for the complete risk matrix):

Feared event	*Levels of severity/likelihood*	*Control measure*	*Residual risk*
Illegitimate access to personal data (confidentiality)	Significant	Disk encryption; TLS; access control;	Low
Unwanted modification of personal data (accuracy and integrity)	Significant	Preservation policies; pseudonymisation	Low
Disappearance of personal data (availability)	Significant	Preservation w/out storage	Low

Table 8: Confidentiality, integrity and availability controls in the PresS

[72] 'Time-lock-encryption' refers to the ability to encrypt data for a specified amount of time. Data can be decrypted only after the expiration of that time, hence assisting in the confidentiality of the (encrypted) data.
[73] Mike Prechtl, Detlef Hühnlein and Andreas Kühne, *D3.4 - Scalable Preservation Service* (final v 1,0, FutureTrust project, 31 May 2017), p. 10.

The PresS adheres to the **necessity** and **proportionality** principles, as it only processes data strictly necessary to perform the preservation (authentication data and electronic signatures, seals and timestamps) and does not impose unnecessary limitations on the data subjects (e.g. by offering a preservation solution without storage of the processed data).

7. FutureTrust Pilot and Demonstrators

7.1 eInvoice Austrian Pilot Application (BRZ)

The objective of the Austrian eInvoice pilot is to demonstrate electronic delivery of eInvoices through automated processes. The scope of the pilot is to support businesses that have registered to access electronic services in Austria (through an electronic portal called the Austrian Business Service Portal – *USP*) by allowing them to submit eInvoices addressed to the Austrian Federal Ministry of Finance (the owner of the *USP* and eInvoice system). The pilot will allow for the submission of eInvoices and related electronic signatures and certificates. The pilot will be using the ValS and gTSL services of FutureTrust to facilitate this functionality.

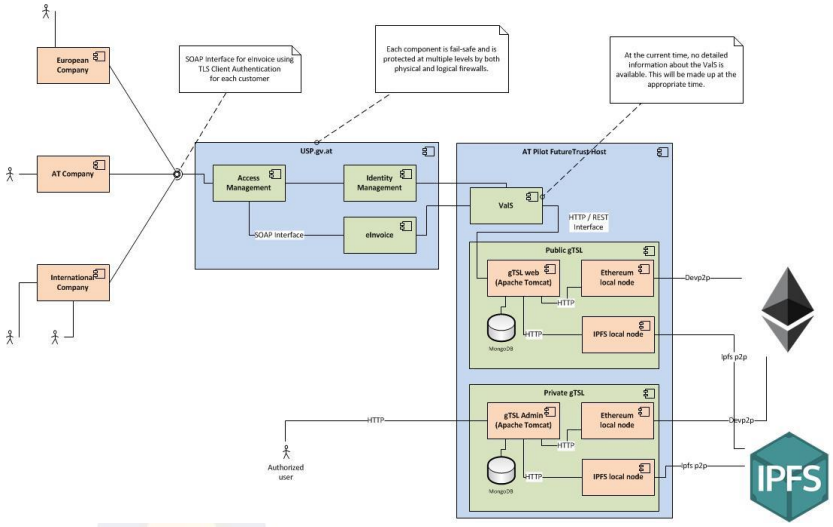


Figure 23: eInvoice pilot application

7.1.1 Stakeholders

The main stakeholders of the eInvoice pilot application are the companies issuing the eInvoices (the pilot partners submitting an expense claim to the Ministry of Finance), the operator of the eGovernment portal (USP) and the FutureTrust services (the ValS and gTSL), which for the pilot is the BRZ, and the Ministry of Finance as the receiver of the invoices.

Some external stakeholders are indirectly involved at the start of the workflow: before being able to submit eInvoices, participating companies must have obtained an electronic certificate and an electronic signature from an organisation issuing trust services. In addition, companies that wish to create test accounts at the USP will need to submit data to the ERsB and ERnP, the "Supplementary Register for other affected parties" and the "Supplementary Register for natural persons". Both registries are owned by the Austrian Data Protection Authority.

For the needs of this pilot, two FutureTrust services are being used: the ValS in order to verify the certificates and signatures and the gTSL, remotely interfaced with the ValS,[74] to verify the trust

[74] Carl-Markus Piswanger and Christoph Zehetner, *D4.9 - Austrian Pilot Service Implementation Documentation* (v11, 28 February 2019), p. 8.

anchors of the certificates and signatures. The two components are hosted in a single host at the BRZ.

7.1.2 Data flows

There are three variations of the data flow to submit an eInvoice, one for already registered users of the USP, one for companies which will register as test users for the needs of the pilot only and one for companies that will not register with USP.

The three versions differ only in the initial step (registration). Companies registered with the USP (or wishing to register with it) need to submit an application to the USP first. The registration process is out of the scope of the pilot, so personal data processing for this process will not be detailed here. Companies that wish to register as a test user for the pilot (second version of the work flow) will need to submit a *company register number* and a copy of the *country specific company registration* along with a *passport copy* of the person authorised to submit eInvoices and a *X.509 certificate* to the USP.[75] After submission they will be issued USP credentials. Submission of eInvoices without prior registration is possible during the phase of the pilot only through the use of an *'eInvoice-transmission-client'*.[76] In the latter case, only uploading of an associated public certificate to the USP is necessary.

After the initial setup, the rest of the data flow is common for all three versions:[77] the company, either through the USP web services or through the transmission client sends a signed eInvoice to the USP. The eInvoice is received by the access management component, which after successful authentication of the sending company forwards the eInvoice to the eInvoice system; in the version specific for the pilot's needs, the verification step is skipped as companies do not need to register. The eInvoice system receives the eInvoice and forwards the signature element and the associated authentication certificate to ValS. ValS looks up the certificate in the gTSL and verifies the signature. The response of the verification is then sent to the eInvoice system, which processes the eInvoice and forwards a receipt to the sending company.

7.1.3 Processing purposes and legal bases

The general purpose of the pilot is to allow companies to bill the Austrian Ministry of Finance for services provided using eInvoices. It should be noted that invoicing the Ministry of Finance is already possible through other means, the pilot will just offer an additional electronic way of invoicing through the use of trust services. Therefore, potential legal bases for the processing can be either the performance of a contract,[78] compliance with legal obligations,[79] the legitimate interests of the controller,[80] or based on consent.[81] For the purposes of the pilot it is assumed that processing will be based on consent.

[75] Ibid, pp. 18-19.
[76] Ibid, p. 9.
[77] Carl-Markus Piswanger and others, *D3.7.1 - eInvoice submission to the Austrian Public Sector using web service authentication and eSignature (AT pilot and demonstrator)* (v11, 31 May 2017), p. 17.
[78] GDPR Art. 6(1)(b).
[79] GDPR Art. 6(1)(c).
[80] GDPR Art. 6(1)(f).
[81] GDPR Art. 6(1)(a).

7.1.4 Personal data processing use cases

Although eInvoice processing is mainly done in the 'eInvoice transaction' sub-process, several sub-processes exist as a pre-requisite. Of them, only one (the "eInvoice transaction") applies when the transmission client is used. In all processes, steps that are performed by a user denote a process performed by the company's authorised representative.

7.1.4.1 Sub process SP-BS-1.1-2 "User Registration" [Optional]

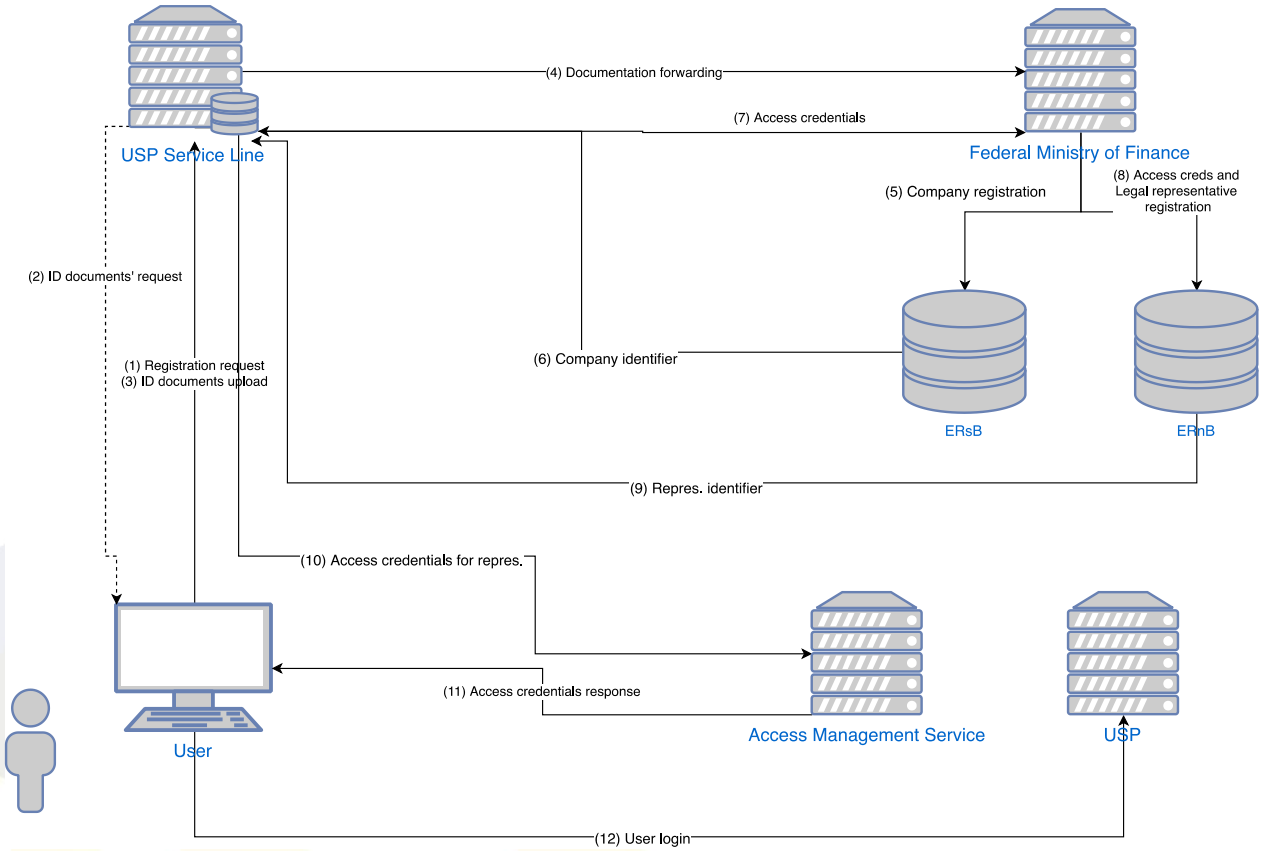


Figure 24: eInvoicing user registration

This process is initiated manually, through contact of the interested user with the USP Service Line. The Service Line sends a request for necessary documentation (copy of company's registration, company's registry ID, copy of representative's passport). The documents are electronically sent by the user to the Service Line, which forwards them to the Federal Ministry of Finance. The Federal Ministry approves the request and sends the organisational information of the company to the ERsB (Registry of companies). The ERsB produces an identifier for the company. The identifier is forwarded to the Service Line, which then produces the access credentials for the representative(s) of the company. The access credentials along with information about the representative are registered at the ERnP (registry of persons). The ERnP produces an identifier, which is forwarded to the Service Line. The Service Line produces login credentials, which are sent to the access management service and forwarded to the user. The user performs an initial login to the USP.

7.1.4.2 Sub process SP-BS-1.1-1 “USP Login” [Optional]

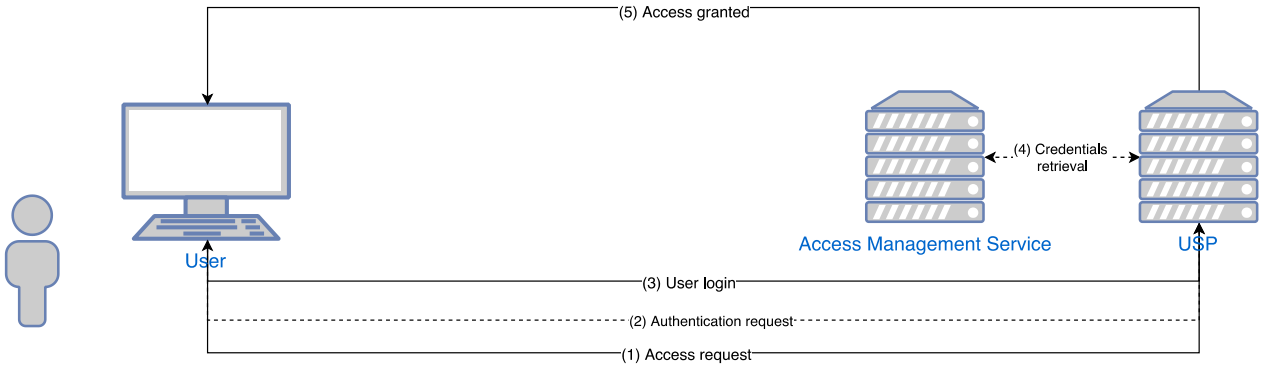


Figure 25: eInvoicing user login

The user accesses the USP through a browser. The USP presents the user with an authentication dialog. The user inputs their credentials which are then checked against the USP’ access management system. If the credentials are valid, the user information is checked against the USP’ LDAP service. If the user has been previously registered, the USP-LDAP logs the user in the USP portal. Otherwise, the user is prompted to register (sub-process above).

7.1.4.3 Sub process SP-BS-1.1-3 “Certificate Upload”

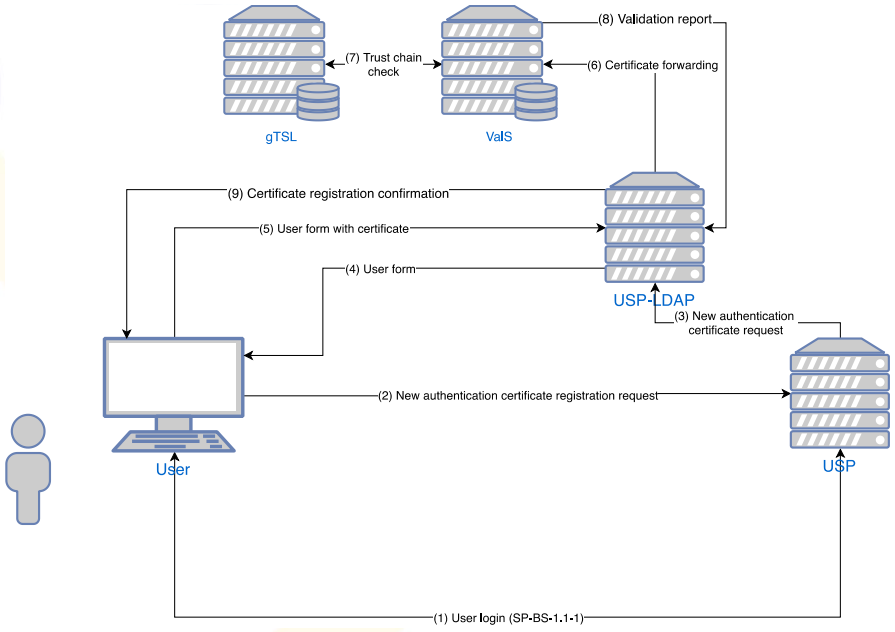


Figure 26: eInvoicing certificate upload

Users wishing to use the eInvoicing service will first need to upload an electronic certificate that will be stored at the USP-LDAP and used to verify the signatures of the eInvoices. After successful access to the USP portal, the user submits a request to upload a new authentication certificate.

The IDM component of the USP delivers a form to the user, allowing them to attach an authentication certificate and send it back to the USP. The IDM forwards the certificate to ValS. The ValS checks the certificate, using process 6.3.4.2. The certificate chain is sent through the ValS to the gTSL, which holds the trust anchors. The gTSL sends back a report on the trust chain. The ValS reports back to the IDM and if no errors are reported the IDM stores the certificate and sends a confirmation of the certificate registration to the user.

7.1.4.4 Sub process SP-BS-1.1-4 “Web Service Administration”

This is a once-only process to assign eInvoicing rights to the user account. The user has to login to the USP, navigate to the user rights settings and enable access for the eInvoice system.[82]

7.1.4.5 Sub process SP-BS-1.1-5 “eInvoice Transaction”

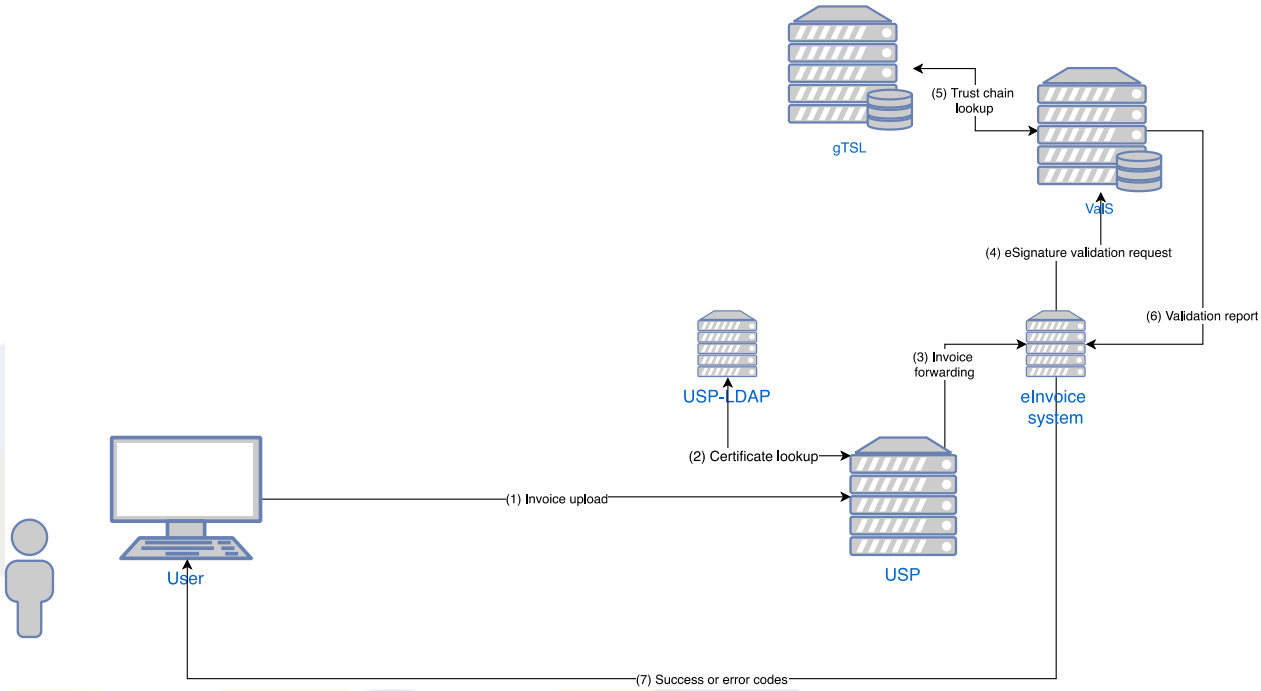


Figure 27: eInvoicing invoice transaction

The main process to submit a new eInvoice for processing is initiated by the user, who either submits a new eInvoice through the USP portal or uses the transmission client. With either of these options, the eInvoice should be accompanied by an electronic signature and an authentication certificate. The USP IDM service looks up for a stored version of the certificate. Upon successful discovery of the certificate, the signed eInvoice is forwarded to the eInvoice system. The eInvoice system sends the electronic signature object to the ValS. The ValS looks up the certificate chain in the gTSL and validates the signature using process 6.3.4.1. The ValS reports the validation to the eInvoice system and a success code back to the user, or a list of technical errors if validation of the eInvoice or the signature was not possible.

[82] Piswanger and Zehetner, *D4.9 - Austrian Pilot Service Implementation Documentation*, n. 74, pp. 21-22.

In the case where only the transmission client is used, the sub- process 7.1.4.5 applies. The transmission client, or 'eInvoice client, is available as a standalone component in github.[83] The basic premises of the process remain the same, but installation and management of the client have been simplified. Interested users need only download the standalone client from the repository and install it, pointing to a key store of their own choosing where appropriate certificates are held. From there on, the process is the same as the one described above.

7.1.5 Data protection roles per use case

Out of the above use cases, not all will process personal data. Hence, only the use cases where personal data are processed will be commented on below. Further, it has been made possible within the pilot for users to submit eInvoices without prior registration, hence without processing for registration or login purposes. However, since under normal use registration will be needed, processing for registration purposes will also be examined below.

The processes of 'USP login', 'Certificate upload' and 'Web Service Administration' are excluded since the data they process concern legal persons and, as such, are outside the scope of the GDPR.

7.1.5.1 Sub process SP-BS-1.1-2 "User Registration" [Optional]

The purpose of processing in this use case is to register the company and its representative in order to access eGovernment services through the business portal – including the eInvoice system. Since this is a process that is required to access any of the offered eGovernment services for businesses in Austria, it is assumed that in most cases (i.e. if the eInvoice system moves into production) businesses that transact with the Austrian government would have already undergone this process.

Two sets of data are processed in this use case: data about the identity of the company (company registry number, country of origin, electronic certificate etc.) and data about the identity of the company's representative(s). Out of the two, only the latter contains personal data: the data contained in the copy of the passport of the representative, i.e. full name, date of birth, passport number, country of origin, citizenship, photograph.

The entity that is responsible for the processing of passport data is the FutureTrust office in the BRZ – a subset of the operator of the USP. So, **the USP is the data controller**. Although the organisation of the Austrian public authorities is out of the scope, if the two registries, the ERsB (to the extent that personal data of the representative are stored here) and ERnP, are operated by a different entity, then **the operator of the registries will act as a data processor on behalf of the BRZ**.

7.1.5.2 Sub process SP-BS-1.1-5 "eInvoice Transaction"

The purpose of this use case is to verify the validity of an eInvoice by an authorised supplier and record the eInvoice for further processing. Two sets of data are processed: the electronic signature and certificate that accompany the eInvoice and the data contained within the document.

To the extent that the eInvoice is signed by an electronic signature and not an electronic seal, the electronic signature will be considered as personal data. Electronic seals, as defined in eIDAS

[83] https://github.com/FutureTrustAT/ft-ac-cc

Article 3(25), are created by and contain data of legal persons and, therefore, are not captured by the GDPR. The signature will be processed by ValS, after instruction by the BRZ. Hence, **the BRZ is the data controller** and, to the extent ValS is operated by a different entity, **the ValS is a data processor on behalf of the BRZ**. The gTSL does not process any personal data.

It should be assumed that some personal data are contained within the eInvoice itself, for accounting purposes. These will vary depending on the specific contents of the eInvoice, but at the very least personal data of the biller and their banking account should be assumed (see Table 9). For the purposes of recording and forwarding the eInvoice for further processing, **the BRZ is the data controller** for the personal data contained within the eInvoice.

```
<eb:Biller>
 <eb:VATIdentificationNumber>ATU13585627</eb:VATIdentificationNumber>
 <eb:Address>
  <eb:Name>Schrauben Willi</eb:Name>
  <eb:Street>Lassallestraße 5</eb:Street>
  <eb:Town>Wien</eb:Town>
  <eb:ZIP>1020</eb:ZIP>
  <eb:Country>Österreich</eb:Country>
  <eb:Phone>+43 / 1 / 78 56 789</eb:Phone>
  <eb:Email>philip.helger@brz.gv.at</eb:Email>
  <eb:Contact>Sachbearbeiter Meier</eb:Contact>
  <eb:AddressExtension>Zentrale Verwaltung Wien</eb:AddressExtension>
 </eb:Address>
 <eb:InvoiceRecipientsBillerID>0011025781</eb:InvoiceRecipientsBillerID>
</eb:Biller>

<eb:PaymentMethod>
 <eb:Comment>Wir ersuchen um termingerechte Bezahlung.</eb:Comment>
 <eb:UniversalBankTransaction>
  <eb:BeneficiaryAccount>
   <eb:BankName>Bank Austria CA</eb:BankName>
   <eb:BankCode eb:BankCodeType="AT">12000</eb:BankCode>
   <eb:BIC>BKAUATWW</eb:BIC>
   <eb:BankAccountNr>11111111111</eb:BankAccountNr>
   <eb:IBAN>AT611904300234573201</eb:IBAN>
```

```
    <eb:BankAccountOwner>Max Mustermann</eb:BankAccountOwner>
   </eb:BeneficiaryAccount>
   <eb:PaymentReference>12345678</eb:PaymentReference>
  </eb:UniversalBankTransaction>
 </eb:PaymentMethod>
```

Table 9: Examples of personal data contained within an eInvoice

7.1.6 Data Protection by Design in the eInvoicing pilot application

The eInvoicing pilot will be processing two sets of personal data: personal data concerning the natural person who acts as a representative for the company and personal data contained within the eInvoice.

The **purpose is limited** to processing that enables the electronic submission of invoices to the Austrian government. The **legal basis** for the pilot will likely be based on consent, and access to the pilot will be granted after successful demonstration of informed consent. The only barriers to entry are existing requirements for companies and their representatives to be registered with the Austrian registries of companies (ERsB and ERnB), in order to use any of the available electronic services of the business portal. Therefore, the pilot adheres to the principle of **fairness**. The **accountability** principle of Article 5(2) is complied with through this report focusing on the pilot along with the privacy assessments of the business portal's services that BRZ conducts internally.

The **confidentiality** of processed data is ensured through cryptography. End-to-end encryption is set up between the FutureTrust components and the business portal. The use of the business portal and the FutureTrust services is secured through access control.

The **accuracy** and **integrity** controls set up in the ValS and the gTSL are supplemented by the registration of the pilot participants to the business registries and manual controls of the submitted eInvoices.

Since the pilot only sets up an electronic way of submitting invoices to the Ministry of Finance (where the actual processing in order to pay the invoices takes place), the pilot uses end-to-end encryption for the submission of the eInvoices and does not store them once their validation has been successful. Therefore, no particular risks to **availability** should exist and the **storage limitation** principle should be considered met. The storage limitation principle is additionally satisfied by the automatic deletion of all personal data from the business registries after the end of the pilot phase, unless the participant has explicitly opted for their data to remain in the registries to retain access to the business portal.

Personal data of the company representative are only collected once upon initial registration and only if the company has not already been registered in the ERsB. In order to forward the eInvoice for financial processing, only the validity of the electronic signature and the format is checked. Therefore, data processing is **minimised** according to the purpose. No further information is held by the pilot, therefore linkability to other uses inside or outside of the business portal is not possible. This is further achieved by the **unlinkability** controls implemented in the ValS (pseudonymisation).

Transparency is served through the privacy notices of the business portal along with a privacy notice that is context specific to the pilot and details the processing, data flows and rights of the data subjects. Aside from the automatic processes to ensure deletion of personal data after the end of the pilot, manual processes exist to allow the data subjects to exercise their rights (**intervenability**).

The table below maps the control measures to the feared events associated with the eInvoicing pilot application. More specifically it describes the potential feared events that, if occurred, would impact the rights and freedoms of the data subjects, the control measures that have been introduced to mitigate the feared events and the residual risk (the likelihood of the feared event taking place *x* the severity of its impact after application of the control measures).

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Unnecessary or unspecified processing (purpose limitation)	Limited	Specified, explicit, legitimate purposes; policies; staff training	Low
Processing not based on a lawful basis (lawfulness)	Limited	Legal ground set in policy; staff training	Low
Discriminatory processing (fairness)	Significant	Participation open to all ERsB/ERnB members	Low
Incomplete or non-existent evidence of processing (accountability)	Limited	DPbD report; DPIA	Low
Excessive processing of data (data minimisation)	Limited	(*see* purpose limitation and unlinkability); pseudonymised identifiers; hash values for validation; stateless operation where possible	Low
Processing for longer than necessary	Limited	Stateless operation where possible; deletion of data after data subject request	Low

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
(storage limitation)		or automatically after pilot end	
Illegitimate access to personal data (confidentiality)	Significant	TLS; disk encryption; access control	Low
Unwanted modification of personal data (accuracy and integrity)	Significant	SSO cache; encryption; manual check of eInvoices; registration of both business and legal representative	Low
Disappearance of personal data (availability)	Significant	End-to-end encryption; disk encryption; stateless operation (processed data passed on Finance)	Low
Unnecessary linkability of attributes and/or uses (unlinkability)	Limited	Pseudonymised unique identifiers; no information held to link to other uses of the Business Portal;	Low
Opaque or vague information on processing (transparency)	Limited	Context specific privacy notice of pilot; privacy notice of Business Portal	Low
Difficult or impossible exercise of data subject rights (intervenability)	Negligible	Processes to exercise data subject rights; manual controls	Low

Only the right to access the pilot and the validity of the submitted eInvoice are checked within the pilot; valid eInvoices are forwarded to the Ministry of Finance. Therefore, the pilot adheres to the principles of **necessity** and **proportionality**.

7.2 SEPA e-Mandates Demonstrator (Multicert)

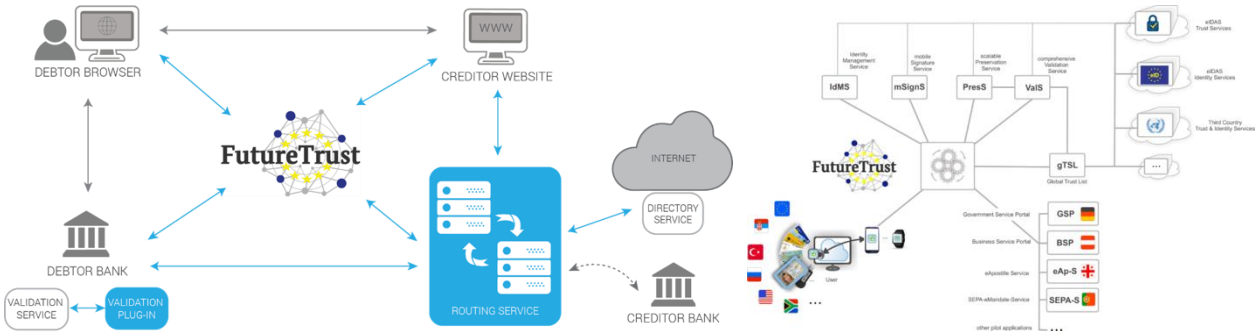


Figure 28: eMandates demonstrator

The objective of the SEPA e-Mandates demonstrator is to replace the paper-based process that is used in the Direct Debit Mandate authorisation between a bank, a consumer and a service. The e-Mandates demonstrator will integrate several of the FutureTrust services (depicted in Figure 28).

7.2.1 Stakeholders

The main stakeholders in the e-Mandates demonstrator are the debtor, the creditor, the debtor's bank and the creditor's bank. The debtor is a user wishing to use a service of the creditor in exchange for remuneration. The creditor is the entity providing the service.

To the above entities, four others must be added: a routing service, which redirects e-Mandate requests to the debtor bank; a validation service, which processes the e-Mandates on behalf of the debtor bank; a directory service, which enables reachability of all participating banks; and, an approved certification authority, that issues certificates for the validation and the routing services. Apart from the certification authority which is an independent entity, the other three entities might be modules of the creditor bank (routing service; directory service) or debtor bank (validation service) or can be third parties that are contracted to provide these services to the creditor and debtor banks.

For the needs of this demonstrator, four FutureTrust services are being used: the IdMS, the mSignS, the ValS and the PresS. The IdMS and mSignS services are integrated into the debtor bank infrastructure. The ValS service can be either integrated into the debtor bank or be a third party service. The PresS is integrated into the creditor infrastructure.

7.2.2 Data flows

The main dataflow, the creation of an e-Mandate, involves all detailed stakeholders. In summary, when a user (debtor) wishes to sign up to a service of a provider (creditor) that requires a direct debit, the user is able to set up an e-Mandate to instruct their bank to credit the provider's account with the amount through the creditor's webpage. To do this, the user will need to fill out a form that will then be used along with the provider's information to construct a request to the user's bank to debit the user's account and send the defined amount of money to the provider's account. The request is sent to the bank, verified as to its validity along with the user's identity and the resulting direct debit report is sent back to the provider. The provider validates that the report is genuine and saves it for future reference. A detailed description of the data flows follows in 7.2.4.

7.2.3 Processing purposes and legal bases

The general purpose of this demonstrator is to allow users (debtors) to set up direct debits with electronic services (creditors) using e-Mandates. Three main data flows are involved in this process: an e-Mandate request, an e-Mandate response and an electronic singing using an electronic certificate. The purpose of the e-Mandate request is to instruct the debtor's bank that the debtor wishes to set up a new direct debit to the creditor. Accordingly, the purpose of the e-Mandate response is to notify the creditor that a new e-Mandate has been successfully set up. The purpose of the electronic signing is to verify the validity of the data contained in the e-Mandate. All cases of personal data processing performed for these purposes are based on user consent: the user is the entity initiating the process, wishing to sign up to a service of the creditor and willing to set up a direct debit through their bank to this end.

7.2.4 Personal data processing use cases

There is a detailed explanation of all possible use cases, divided into targeted entities (creditor portal; debtor bank) in D3.7.4.[84] For the purposes of this report, use cases that correspond to one process from the debtor's (the user's) point of view have been combined. As a result, there are three possible scenarios where personal data will be transmitted: Login authentication against the creditor portal; login authentication against the debtor bank; create and submit mandate on the creditor portal.[85] Below they are presented simplified, with a focus on the personal data flows.

7.2.4.1 Login authentication on the creditor portal

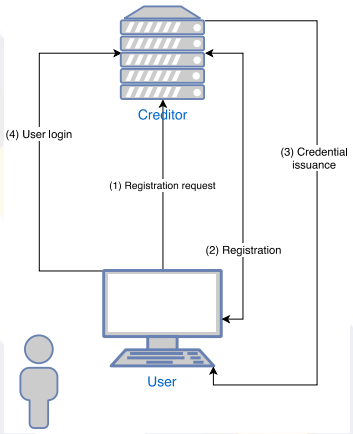


Figure 29: e-Mandates creditor portal login

The creditor portal is the website set up by the creditor where the debtor (the user) can sign up for one of the offered services. Login at the portal happens via username and password, after a successful registration process. The registration process will vary for different creditors, as each creditor is in charge of determining what information are needed to successfully register a user. At the very minimum, though, it should be considered that the user will have to submit a valid email address and their real name, select a username and

[84] Carlos Cardoso and others, *D3.7.4 - SEPA e-Mandates Demonstrator* (v10, 16 May 2017), pp. 25—38.
[85] Which will then trigger one of three processes on the debtor bank: authorize mandate with or without signature and cancel mandate.

create a password. This information is stored on the creditor's database, at least for as long as the user is signed up for one of their services.

Therefore, when a debtor wishes to either create a new mandate or query the status of an old one, the debtor accesses the creditor portal through their browser. The creditor portal requests an authentication. The user fills in their credentials. The creditor portal queries their database and upon successful retrieval of the credentials logs the debtor in.

7.2.4.2 Login authentication on the debtor bank

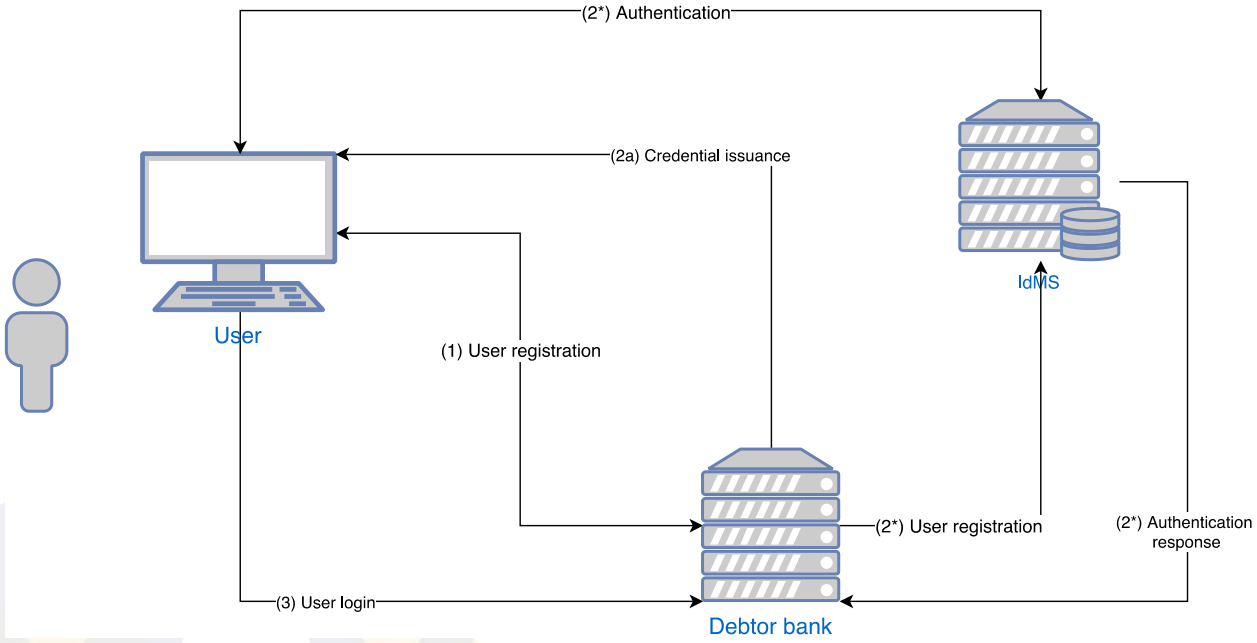


Figure 30: e-Mandates debtor bank login

Again, the process is dependent on prior successful registration of the debtor with the debtor bank. The information needed for the registration are dependent upon the bank's policies, in line with applicable legislation.

There are two possible scenarios to login to the debtor bank:

1. Logging in using the authentication method provided by the debtor bank. This can be a username and password supplied by the bank, or coupled with a two-factor authentication (using a hardware module supplied by the bank or a mobile device). In this case, only the personal data held by the bank are accessed (usually a username and a password).
2. Logging in using IdMS single sign-on via a smart-card. The debtor clicks on an "ID" button on the bank's webpage. The debtor presents their smart card on the reader attached to their computer. The smart card contains a personal certificate, with the debtor's eID data. A request for authentication is sent to the IdMS (located at the debtor bank). Use case 6.1.4.1 is followed. An attestation with the debtor's minimum dataset (name, date of birth, unique identifier) is returned to the debtor bank. The debtor bank matches the dataset to a client record and logs in the debtor.

7.2.4.3 Create and submit mandate

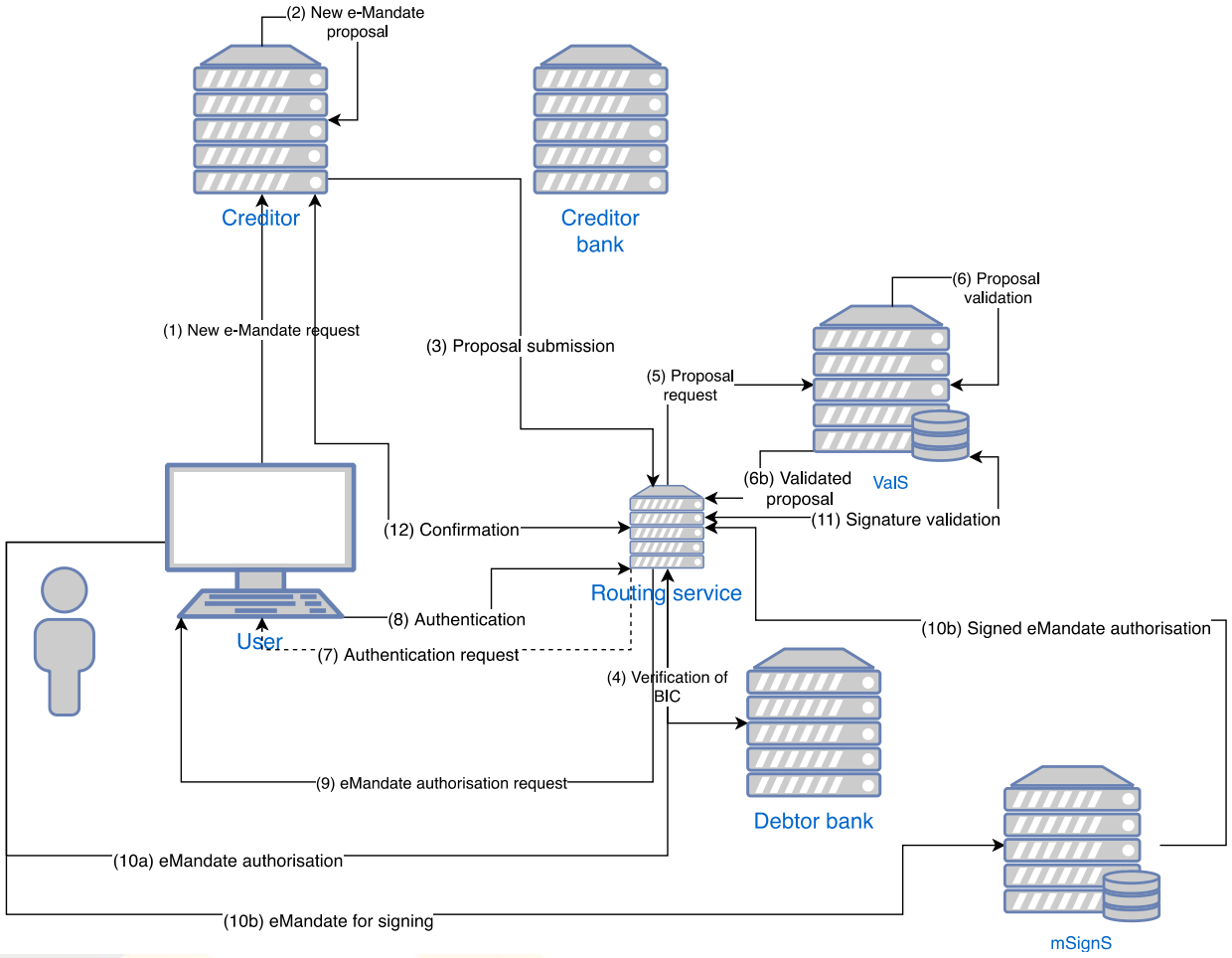


Figure 31: e-Mandates new mandate creation

After successful log in to the creditor's portal, the debtor opts to create a new e-Mandate. The creditor's portal presents a form to the debtor's browser. The debtor fills in the form with their information. The information needed might change from creditor to creditor, but it is at least assumed that the name, address, date of birth, place of birth and the debtor bank's SWIFT BIC code are the maximum amount of data required. The debtor submits the form to the creditor.

The creditor's portal merges the data submitted with data about the creditor and creates a new e-Mandate proposal. The proposal is submitted to the routing service (housed at the debtor bank or at a third-party entity). The routing service verifies the creditor's credentials and looks up in the directory service the operational BIC of the debtor's bank. The directory service returns the URL of the debtor's bank to the routing service. The routing service then submits the proposal as a request to the validation service of the debtor bank using the supplied URL. Both the routing service and the validation service must present valid certificates from a certificate authority. The validation service validates the request and redirects the debtor's browser to the debtor bank, where the user performs a log-in.

After successful authentication to the bank, the debtor is presented with the mandate proposal. The debtor can then authorise the proposal either with or without an electronic signature. If the debtor opts to authorise the proposal with a signature, the mSignS process 6.3.4.1 or 6.3.4.2 is followed. The mSignS then affixes the produced electronic signature to the e-Mandate and the signed mandate is sent to the debtor bank validation service. The validation service verifies the authorisation and electronically signs the e-Mandate data on the envelope message. The validation service presents a confirmation message to the debtor's browser with a link to return to the creditor's portal. The debtor follows the link to the creditor's portal. The creditor's portal retrieves the e-Mandate through the routing service and presents a confirmation message to the debtor. The signed e-Mandate data are stored at the creditor's database and forwards an acknowledgement of receipt via the routing service to the validation service. The signed e-Mandate is preserved on the PresS, following process 6.5.4.1.

7.2.5 Data protection roles per use case

7.2.5.1 Login authentication on the creditor portal

The purpose of the processing here is to authenticate a registered user. There are two separate data flows, one for the registration of the user and one for subsequent authentication. For both processes the entity that determines the means and purposes of processing is the creditor. Hence, **the creditor is the data controller**, with the debtor (the user) being the data subject.

7.2.5.2 Login authentication on the debtor bank

The purpose of the processing is to authenticate a previously registered user (client of the bank; registration of the debtor with the bank is out of scope since it is assumed that the debtor already holds an account with the bank). The debtor bank is the entity that requires authentication to allow access to the services. Therefore, the debtor bank is determining the purposes of processing. The debtor might be able to select a means of authentication they wish to use, but the list of available means is determined by the debtor bank. Hence, the means should also be considered to be determined by the debtor bank. The **debtor bank is the data controller**, with the debtor being the data subject.

7.2.5.3 Create and submit mandate

The purpose is to create a new e-Mandate. The purpose is determined by the creditor, since the creditor is the entity that decides that in order to provide a service a mandate is required. Processing of personal data is happening in three different entities: the creditor's portal, the debtor bank and the creditor bank. However, the means (the data of the e-Mandate, the form used to fill them in, the electronic signatures required to be considered valid) is still determined by the creditor. Hence, **the creditor is a data controller**. The debtor bank is validating the e-Mandate proposal after request of the creditor, with the consent of the user. However, the debtor bank is determining the means of the validation (successful authentication with one of the pre-determined means, consent of the debtor). Hence, even though the debtor bank is responding to a request from the creditor, **the debtor bank should also be considered a controller**. According to Article 29 Working Party, controllership can arise when a party determines either the purpose or "*those*

essential elements of the means".[86] Accordingly, **the routing, validation, IdMS, mSignS and PresS services also perform processing as data processors** on behalf of the creditor.

7.2.6 Data Protection by Design in the e-Mandates

The eMandates demonstrator will be processing three sets of personal data: personal data concerning the natural person who wishes to submit an eMandate, including authentication data of that person to the service provider, authentication data of the service provider to the debtor bank and personal data contained within the eMandate. For the purposes of the demonstrator, the service provider and the banks will be mock-ups, therefore processing that is performed by them will be skipped.

The **purpose is limited** to processing that enables requests of new eMandates to be passed on to the user's bank and a confirmation of their successful set up back to the service provider. The **legal basis** for the demonstrator is based on consent, and access to the routing service will be granted after successful demonstration of informed consent. Criteria for eligibility are that the user is using an eID means that is either notified under eIDAS or from a country with a known profile to the IdMS; since the SigS and the ValS can be used to enhance eID means to support electronic signing. Even users with no previous means to e-sign can use the demonstrator. Therefore, the pilot adheres to the principle of **fairness**. The **accountability** principle of Article 5(2) is complied with through this report focusing on the pilot along with the privacy assessments performed by Multicert internally about their infrastructure.

The **confidentiality** of processed data is ensured through cryptography. End-to-end encryption is set up between the FutureTrust components and the routing service. The use of the routing service and the FutureTrust services is secured through access control and confidentiality is further assured through audit trails.

The **accuracy** and **integrity** controls set up in the ValS and the gTSL are supplemented by audit trails and SSL/TLS certificates.

No particular risks to **availability** shall exist since the routing service does not store any data once the eMandate request and its confirmation have been forwarded. For the same reason, the **storage limitation** principle should be considered adhered to. The storage limitation principle is additionally satisfied by the automatic deletion of all personal data after the end of the demonstrator.

The stateless operation of the routing service, along with the pseudonymisation and hashing controls of the FutureTrust services supports **data minimisation**. No further information is held

[86] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169, adopted on 16 February 2010), p. 19; see also p. 14: "*Determination of the "means" therefore includes both technical and organizational questions where the decision can be well delegated to processors (as e.g. "which hardware or software shall be used?") and essential elements which are traditionally and inherently reserved to the determination of the controller, such as "which data shall be processed?", "for how long shall they be processed?", "who shall have access to them?", and so on. Against this background, while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means.*" Of the same opinion the recent Opinion of Advocate General Bot on 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, EU:C:2017:796, para. 62.

by the demonstrator, and the routing service can function as a broker between the service provider and the bank to mask their identity from one another. Therefore, **unlinkability** controls are implemented, enriched by the controls existing in the IdMS, the SigS, the ValS and the PresS.

Transparency is served through the context specific privacy notice that details the processing, data flows and rights of the data subjects. Aside from the automatic processes to ensure deletion of personal data after the end of the pilot, manual processes exist to allow the data subjects to exercise their rights (**intervenability**).

The table below maps the control measures to the feared events associated with the eMandates demonstrator. More specifically it describes the potential feared events that, if occurred, would impact the rights and freedoms of the data subjects, the control measures that have been introduced to mitigate the feared events and the residual risk (the likelihood of the feared event taking place *x* the severity of its impact after application of the control measures).

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Unnecessary or unspecified processing (purpose limitation)	Limited	Specified, explicit, legitimate purposes; policies; staff training	Low
Processing not based on a lawful basis (legal basis)	Limited	Legal ground set in policy; staff training	Low
Discriminatory processing (fairness)	Significant	Supported eIDs through country profiles; e-signing through mSignS or ValS to include all possible eID means; debtor and bank mockups accessible to all participants	Low
Incomplete or nonexistent evidence of processing (accountability)	Limited	DPbD report; DPIA	Low

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Excessive processing of data (data minimisation)	Limited	(*see* purpose limitation and unlinkability); pseudonymisation; hash values for validation; stateless operation where possible	Low
Processing for longer than necessary (storage limitation)	Limited	Stateless operation where possible; deletion of data after data subject request or automatically after pilot end	Low
Illegitimate access to personal data (confidentiality)	Significant	SSL/TLS certificates; disk encryption; access control; audit trails	Low
Unwanted modification of personal data (accuracy and integrity)	Significant	SSL/TLS certificates; audit trails	Low
Disappearance of personal data (availability)	Significant	End-to-end encryption; disk encryption; stateless operation (routing service)	Low
Unnecessary linkability of attributes and/or uses (unlinkability)	Limited	Pseudonymisation; routing service as a broker (blind providers);	Low
Opaque or vague information on processing (transparency)	Limited	Context specific privacy notice of demonstrator	Low

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Difficult or impossible exercise of data subject rights (intervenability)	Negligible	Processes to exercise data subject rights	Low

The main component of the demonstrator, the routing service, only processes the information necessary to forward the request to set up a new eMandate and a successful confirmation. Therefore, the demonstrator adheres to the principles of **necessity** and **proportionality**.

7.3 e-Apostille Verification System (PSDA)

The e-Apostille demonstrator aims at providing an alternative to paper-based apostilling and legalisation services for official documents. The demonstrator builds upon the probative value given to electronic signatures by eIDAS when the latter are used by governmental entities or notaries to verify the authenticity of a document in an electronic form (even though the birthing documents might be in any format, paper-based or not). To that goal, the demonstrator is employing the ValS created by FutureTrust to verify the validity of the affixed electronic signatures, but also using the gTSL, the IdMS and the PreS in the process.

The demonstrator will test the verification of apostille documents for the state of Georgia (where PSDA is the issuing body). Georgia is not a member of the EU, and it is not currently covered by an adequacy decision.[87] Hence, if data are to be exchanged between an EU Member State and Georgia, Georgia will be considered a third country for data protection purposes. However, for the scope of this demonstrator, no personal data will be exchanged outside of Georgia's territory. Even though the Georgian data protection laws are applicable for this scenario, the analysis that follows will be based on the GDPR since the demonstrator aims to test services that will be operated by EU Member States as well.

7.3.1 Stakeholders

There are four main entities participating in the demonstrator: the body issuing the apostille document (in this demonstrator the PSDA); bodies verifying the authenticity of the originating documents (in this demonstrator the National Centre for Educational Quality Enhancement of Georgia and the Service Agency of the Ministry of Internal Affairs of Georgia); the relying parties in the same or other states (the bodies requesting the apostille – in the demonstrator this will be the PSDA); and, the data subject (the citizen whose documents are legalised/apostilled).

The FutureTrust services that will operate in this demonstrator (the IdMS, the PresS, the ValS) can be either integrated into the entity issuing the validation or be third party services. For the purpose of this demonstrator they will be integrated into the PSDA infrastructure. The gTSL service will be a third party. For the purposes of this demonstrator a test instance of the gTSL will be deployed at the PSDA premises.

To the above, another set of stakeholders should be considered: a sub-group of PSDA employees that will act as administrators for the e-Apostille system.

7.3.2 Data flows

Detailed data flows follow. The generic process involves four entities: the data subject, supplying a relying party with an apostille document; the relying party wishing to verify the validity of the apostille; the body performing the validation (the PSDA); and, the issuer of the apostille verifying its status.

The validation starts by the relying body who requests a validation to a supplied document. The relying party uploads the document to the PSDA. The PSDA queries the issuing body of the

[87] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

apostille, which responds with the status of the apostille considered as valid or not. The PSDA stores the validation result and displays itto the relying party.

7.3.3 Processing purposes and legal bases

The overall purpose of the e-Apostille demonstrator is to verify the existence and validity of an apostille status of a document. Even though the means of verification are determined by the PSDA which operates the e-Apostille service, the purpose is determined by the body that requests the validation, i.e. the relying party initiating the validation process. Hence, the legal basis of the processing will be determined by the relying party. It is hard to determine beforehand what the legal basis will be without knowing the particulars of why an apostille is needed. However, it can be assumed that at the very least the process is initiated with the consent of the data subject, the citizen, that is, who uploads the document containing the apostille.

For processing on the personal data of PSDA's employees (the administrators of the demonstrator), the basis will depend on the policies of the PSDA, but it is likely to be based on the performance of the employment contract or the legitimate interests of the PSDA.

7.3.4 Personal data processing use cases

7.3.4.1 Validate document

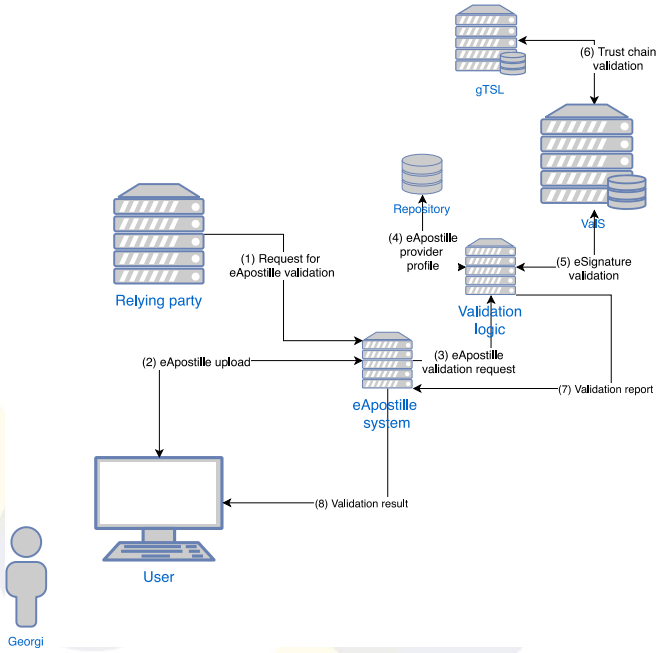


Figure 32: eApostille validation

The process starts by an external user (belonging to a relying party that requests a verification of the apostille for a document of a citizen), who submits a document to the system for apostille. The document should already carry an electronic signature/seal of the body that has carried out the apostille. A 'validation logic bundle' takes over. The bundle queries an internal repository to determine if the provider of the electronic signature/seal is an apostille provider. If the ID of the provider cannot be automatically determined, the system asks for user input. The ValS service, situated in the validation logic bundle, verifies the existence and validity of the electronic signature/seal according to process 6.3.4.1, querying the gTSL in case the signature/seal is

chained to an anchor there. In most cases it is expected that the signature object can be extracted from the document. In these cases only the signature object of the document is checked by the ValS, so the document is not transmitted. If the issuer of the apostille has known formatting rules, the system then checks the endorsement of the document against them. The validation result is displayed to the user. Hence, validation will only exceptionally process any data contained within the document. In most cases, only the electronic signature/seal belonging to a legal person will be checked. In this case, no personal data shall be processed.[88]

7.3.4.1 View list of stored documents and store/open stored document

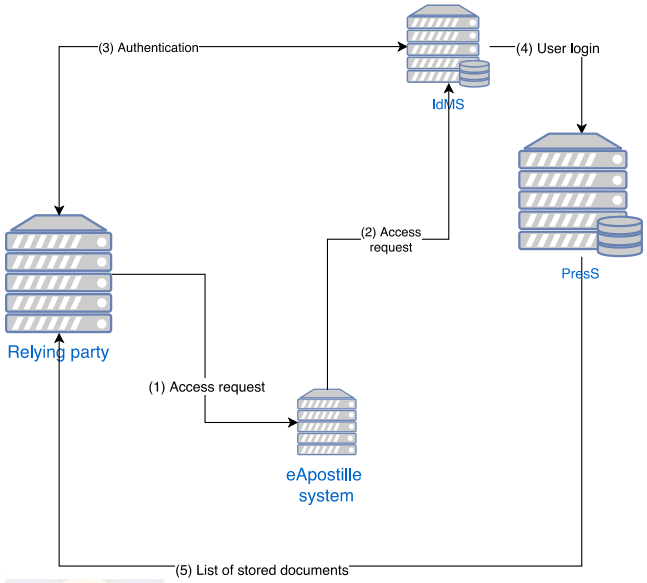


Figure 33: eApostille stored documents

Users of the service (relying parties requesting verification of an apostille) have the option to store documents on the PresS service, to perform validation at a later stage. The option to store a document is presented at the end of the validation process, following process 6.5.4.1, in order to allow for storage of the proof of the validation or in case validation failed the first time. The user can access stored documents after logging in to the PresS service. Logging in is performed through the IdMS service, following process 6.1.4.1 or 6.1.4.3. After successful authentication, the user is presented with a list of the documents they have previously stored in the system along with their preservation status. From there, they can perform a validation as described above of one of the documents.

Since the whole document is stored in PresS, there is the possibility that the document contains personal data. Storage of apostille documents is the only processing of personal data performed within this demonstrator (with the exception of the personal data held for administrator accounts, see below).

[88] Legal persons are out of the scope of the GDPR.

7.3.4.2 Add/edit/delete/view registered provider

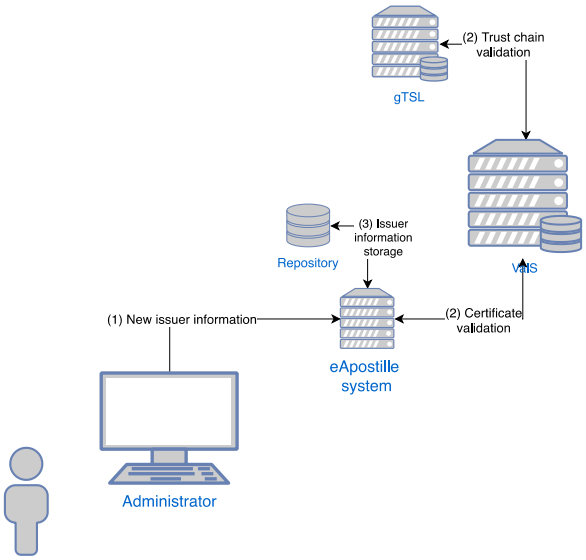


Figure 34: eApostille registered providers

This is part of the administration functionality. Authorised administrators can control which providers are considered as apostille providers. The process starts with an administrator who receives new information about an apostille issuer (either a new issuer, new formatting requirements for an issuer or the cessation of an issuer). The administrator logs into the system to a web-based management interface. The administrator inputs the new data. In case of a new issuer, the administrator can enter, if provided, the URL of the Apostille Status Responder, situated at the issuer, where the issuer is providing information about the status of the apostille documents. The configuration is accompanied by a corresponding certificate that is checked through ValS against the gTSL.

Although this process does not process personal data for the providers, in order for a user to exercise administrator rights, some personal data need to be processed to verify the account in question belongs to the administrator group (username and password, data held in the account's record in the database of users).

7.3.5 Data protection roles per use case

Since there are only three cases where personal data are processed, only these use cases will be commented on below.

7.3.5.1 Validate document

Personal data processing is performed here only in case the system is unable to extract just the signature object from the document. In this case, the whole document is sent to the issuer of the apostille. The processing purpose here is to verify the existence and validity of the signature. The legal basis for the processing of the document is user consent, which is given to the relying party that requests the validation of the apostille. Here the purpose is determined by the relying party (the body that requests the validation of the apostille). The means, however, are determined by the PSDA (the body performing the validation). It should, therefore, be considered that both the **relying party and the PSDA act as joint controllers**. The ValS, PresS, gTSL and IdMS service will be external services, unless they are situated within the PSDA. If they are external services,

they will be data processors acting on behalf of the PSDA. Obviously they will hold the same role as the PSDA if they are integrated within its infrastructure.

7.3.5.2 View list of stored documents and store/open stored document

Personal data processing is performed if a document is stored or retrieved from storage in PresS. The purpose of the processing is the long-term storage of the apostille document and it is determined by the relying party who requests the validation check of the document. The means are determined by the party operating the PresS, hence the PSDA. **The relying party and the PSDA are joint controllers**, whereas if the PresS is situated in an external service, **the eternal service is a data processor acting on behalf of the PSDA**.

7.3.5.3 Add/edit/delete/view registered provider

Personal data processing is performed only in respect of the users that belong to the administrator group. Here the purpose of the processing is to confer certain user accounts with administrative rights. The purpose and the means of the processing are determined by the PSDA (the employer). **The PSDA is a data controller** in respect to the processing of administrators' personal data, whereas the administrators are the data subjects.

7.3.6 Data Protection by Design in the e-Apostille demonstrator

The e-Apostille demonstrator will be processing two sets of personal data: authentication data for the users and personal data contained within the apostille.

The **purpose is limited** to processing in order to validate an e-Apostille. The **legal basis** for the demonstrator will be based on consent. Criteria for eligibility are only the format of the apostille, which has to be one of the supported recognised formats. Unrecognised formats can be submitted to the demonstrator for support. Therefore, the pilot adheres to the principle of **fairness**, since any user that holds a valid eID means can participate. The **accountability** principle of Article 5(2) is complied with through this report focusing on the pilot along with the privacy assessments performed by PSDA internally about their infrastructure.

The **confidentiality** of processed data is ensured through cryptography. End-to-end encryption is set up between the FutureTrust components and the e-Apostille service. The use of the service and the FutureTrust services is secured through access control and confidentiality is further assured through mutual authentication between the components and manual code review.

The **accuracy** and **integrity** controls set up in the ValS and the gTSL are supplemented by the security policies set up at the PSDA and the prevention of public access to the admin interface of the service.

No particular risks to **availability** exist since the e-Apostille and its validation logic do not store any data after validation of the apostille. For the same reason, the **storage limitation** principle should be considered adhered to. If the user opts to store the validated apostille online, storage is protected by encryption. The storage limitation principle is additionally satisfied by the automatic deletion of all personal data after the end of the demonstrator.

The stateless operation of the routing service, along with the pseudonymisation and hashing controls of the FutureTrust services supports **data minimisation**. No further information is held by the demonstrator. Aside from the **unlinkability** controls implemented in the IdMS, the SigS,

the ValS and the PresS, a separation between the development and the operation of the e-Apostille service is implemented as an additional control.

Transparency is served through the privacy notice that details the processing, data flows and rights of the data subjects. Aside from the automatic processes to ensure deletion of personal data after the end of the pilot, manual processes exist to allow the data subjects to exercise their rights (**intervenability**).

The table below maps the control measures to the feared events associated with the e-Apostille demonstrator. More specifically it describes the potential feared events that, if occurred, would impact the rights and freedoms of the data subjects, the control measures that have been introduced to mitigate the feared events and the residual risk (the likelihood of the feared event taking place *x* the severity of its impact after application of the control measures).

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Unnecessary or unspecified processing (purpose limitation)	Limited	Specified, explicit, legitimate purposes; policies; staff training	Low
Processing not based on a lawful basis (legal basis)	Limited	Legal ground set in policy; staff training	Low
Discriminatory processing (fairness)	Significant	Supported eIDs through country profiles; e-signing through mSignS or ValS to include all possible eID means;	Low
Incomplete or nonexistent evidence of processing (accountability)	Limited	DPbD report; DPIA	Low

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Excessive processing of data (data minimisation)	Limited	(*see* purpose limitation and unlinkability); pseudonymisation; hash values for validation; stateless operation where possible	Low
Processing for longer than necessary (storage limitation)	Limited	Stateless operation where possible; deletion of data after data subject request or automatically after pilot end	Low
Illegitimate access to personal data (confidentiality)	Significant	SSL/TLS certificates; disk encryption; access control; source code review; authentication between eAP-S and PresS; security policy	Low
Unwanted modification of personal data (accuracy and integrity)	Significant	SSL/TLS certificates; PSDA security policies; no public access to admin interface	Low
Disappearance of personal data (availability)	Significant	End-to-end encryption; disk encryption;	Low
Unnecessary linkability of attributes and/or uses (unlinkability)	Limited	Pseudonymisation; separation between developers and operation staff	Low
Opaque or vague information on processing (transparency)	Limited	Context specific privacy notice of pilot	Low

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Difficult or impossible exercise of data subject rights (intervenability)	Negligible	Processes to exercise data subject rights	Low

The demonstrator only processes the signature objects (the electronic signature that attests to the validity of the apostille). Authentication of the user is optional, only for the users that opt in to store validated documents online. Therefore, by default the demonstrator adheres to the principles of **necessity** and **proportionality**.

7.4 Smart Certificate Enrolment pilot (Coburg University)

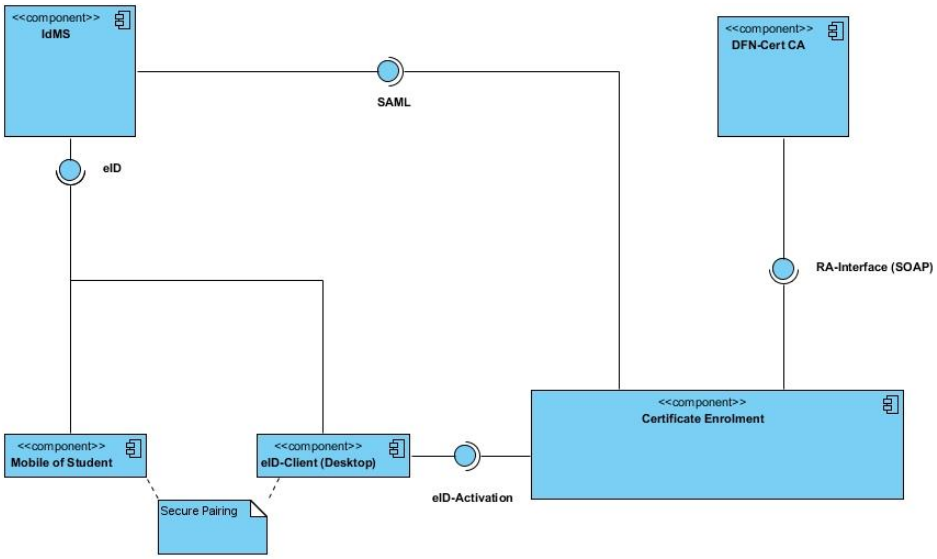


Figure 35: Smart Certificate Enrolment

The objective of the pilot is to showcase, in conjunction with the Coburg University, the use of supported eID means for the creation of electronic certificates issued by professional bodies (in this case the German National Research and Education Network (DFN)). The produced DFN certificates prove membership to the DFN and can be further used to create electronic signatures, encrypt emails or be used by other eGovernment services.

For this purpose, the pilot develops a smart certificate Enrolment Service that will replace the manual process currently followed. The pilot will use the IdMS component of FutureTrust to enrol users and the SigS and PresS components to showcase the use of the produced smart certificates for electronic signatures and email encryption.

As this assessment is commissioned before the end of the project, and while the signing and encryption capabilities of the pilot are still in development, the use of certificates for electronic signing and email encryption will not be assessed in the present document. However, additional information on the data protection safeguards of the FutureTrust components involve can be found in sections 6.2 and 6.5.

7.4.1 Stakeholders

The main entities involved in this pilotare Coburg University which will operate the Certificate Enrolment component and the IdMS and the students or staff participants who are the users of the service. Additionally, the DFN certification authority will be issuing the smart certificates.

For the creation and use of electronic signatures, the SigS component will be used by the users of the service, i.e. the students and staff supplied with a smart certificate.

7.4.2 Data flows

Two main data flows can be identified: a data flow for issuance of a smart certificate and a data flow for use of the certificate to electronically sign a document.

In order to issue a new smart certificate, a member of the DFN (i.e. a student or staff member of Coburg University) will need to enrol first. The user applies for a new smart certificate at the online portal. The portal requests the user to authenticate using their eID card. The user can either use the eID card with a desktop client at their computer (process 6.1.4.1) or use the eID credentials stored on their paired smartphone through the FIDO enrolment (process 6.1.4.2). The result of a successful authentication is then forwarded from the IdMS to the Certificate Enrolment component. The Certificate Enrolment communicates with the DFN-Cert CA, which issues a smart certificate for the enrolled user. The public key is stored at the DFN-Cert CA, whereas the private key is forwarded to the user.

Produced smart certificates will then be used to electronically sign the grading forms used in Coburg University. A user in possession of a smart certificate will use SigS to first authenticate through their eID (as per 6.2.4.1) and then sign the grading forms through an extra component, developed in the form of an application, that accepts PDF documents as input and produces signed PDF documents (through the application-centric process of 6.2.4.2).

7.4.3 Processing purposes and legal bases

For the production of the smart certificates, the purpose is to issue a smart certificate that proves membership to the DFN, through the user's membership to the Coburg University. The relationship between the users, the University and the DFN is contractual.[89] Therefore, processing of personal data for the purpose of this pilotwill likely be based on performance of a contract.

It is noteworthy that the manual equivalent of this process, where University staff check a physical ID and request a certificate from DFN is already in place. The addition of this pilot is the automation of this process by allowing electronic identification of the user. Therefore, it could be argued that there are grounds to allow user consent to be used as a legal basis. User consent is likely to be the legal basis for the optional processing in this pilot, namely if a user opts to store a backup of their certificate to the University's servers.

[89] See Christian Karsch, D4.10 German Pilot (Design Documentation, v 1,0, FutureTrust project, 22 June 2019), p. 7.

7.4.4 Personal data processing use cases

7.4.4.1 Create certificate through eID

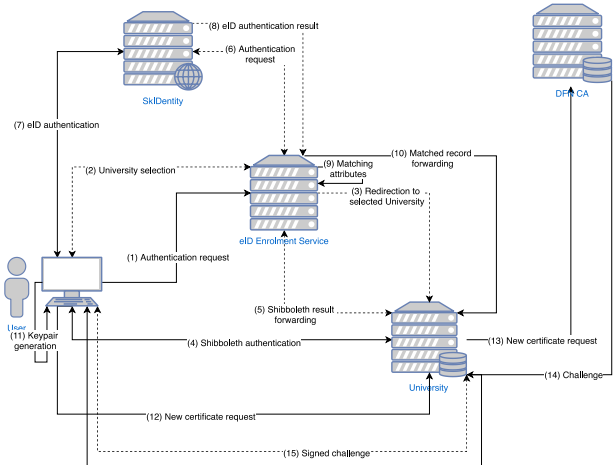


Figure 36: Certificate creation through eID

To perform identification proofing through eID the user visits the eID Enrolment Service. They select their home University and authenticate through their University's Shibboleth authentication page. Upon successful authentication, the user is forwarded to SkIDentity and is asked to perform an authentication using their eID means. If the authentication is successful, the eID Enrolment Service is matching the attributes of the eID means to the attributes of the Shibboleth record. In case of an error in matching the user is advised to contact their University's Service Desk. The user is then asked to enter their telephone number and the matched attributes and telephone number are forwarded to the University.

Next a keypair is generated in SigS located at the user's machine, either through WebCrypto or through CSR. The keypair is sent to the backend with a request for a new certificate. The backend, located at the University, checks the account permissions and sends the request with its parameters to the DFN CA. The DFN CA sends a challenge to the backend which forwards it to user's SigS, and the SigS signs it with the user's private key. The signed challenge is sent back to the backend. If the private and public keys match, the backend issues a new certificate and sends it back to the user.

7.4.4.2 Create certificate with previously proven identity

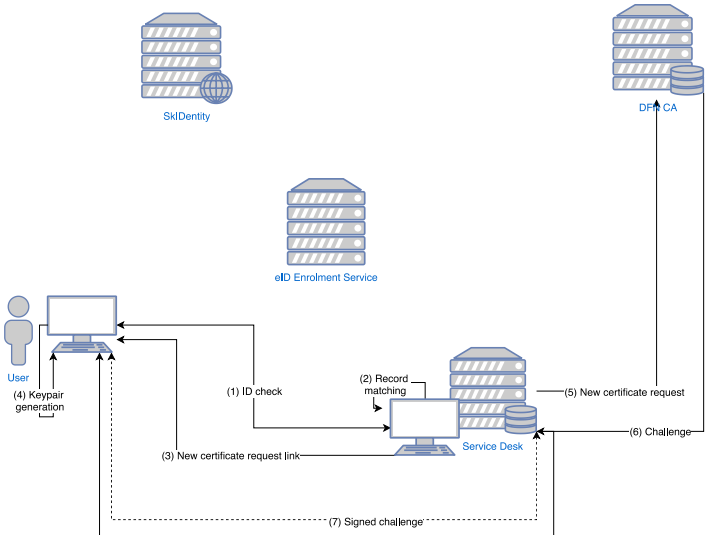


Figure 37: Certificate creation through manual check

Users have the opportunity to prove their identity through a manual check, performed by University staff. The user will have to visit the University's Service Desk and present their ID document. A Service Desk employee looks up the student/staff record in the University's directory and manually checks the provided ID document for matching. The employee then declares the ID check through an attribute at the user's record and stores the user's telephone number if that hasn't already been provided.

After the manual check the user has the option to either request a certificate using their own machine, or request a certificate through the Service Desk and store it on removable media (e.g. a USB stick).

If the user wishes to perform the certificate request on their own, the Service Desk sends the user a link. After clicking on the link, the process continues as above, with the SigS generating a keypair, which is then sent over to the University and used to create a challenge from the DFN CA that when signed by the SigS is matched to the keypair stored at the University. If the keys match, a new certificate is sent to the user.

If the user opts to have the Service Desk request the certificate, then the user's SigS is used only to sign a SAML assertion of the data entered manually by the Service Desk. The keypair is created by the Service Desk and once the certificate is created and sent to the Service Desk, it is saved in a removable medium and given to the user. Because the user's SigS was used to initially sign the SAML assertion, the keypair and certificate are unique to the user.

7.4.4.3 Certificate management

Additional options are given by the front-end for the management of the certificates. The users are presented with a list of their issued certificates and have the option to revoke them. If the user has opted for the optional storage of a certificate at the University's backup storage, they also have options to download a copy of the certificate or download the backup key. The backup decryption key is stored at a hardware token (e.g. a Smart Card), but this functionality is out of the scope of the pilot.

7.4.4.4 Auditing

The identification results, the authentication results and the certificate issuance are logged by the Enrolment Service in audit logs. The audit files, which are represented in XML, contain the SAML assertions and, for the manual identity verification case, the assertion of the administrative personnel. For certificate issuance logs, there is also the certificate of the user logged. The second authentication factor of the user (i.e. the user's phone) is also logged. After the end of each process, the log is timestamped by the Enrolment Service and sent to the University.

7.4.5 Data protection roles per use case

Within this pilot, personal data processing is performed in order to match an eID to a student/staff record. The processing purpose is to issue and manage a smart certificate as a member of the University. Three entities are involved: the user, the University and the DFN. The University can either host an integrated Enrolment Service, or use an Enrolment Service provided by a third party (e.g. a party that operated an instance of SkIDentity).

Although the overall purpose is the issuance of a smart certificate, two separate processing operations (and therefore processing sub-purposes) can be distinguished to this end: processing that is required to confirm that the user is a member of the University; and, processing that is required to electronically confirm the identity of the user. Processing for membership confirmation is already in place through Shibboleth. Processing for verification of identity attributes is also in place, when this verification is performed through manual checks. Processing for electronic verification of identity attributes is first introduced by this pilot, and performed by the Enrolment Service. Finally, processing is also performed in managing issued certificates, to adhere to data subjects' exercise of rights (access, erasure, portability etc.).

7.4.5.1 Create certificate through eID

In this scenario, processing is undertaken by the Shibboleth component of the University to confirm the user's membership. Additionally, processing is undertaken by the Enrolment Service to match the user's membership information (student/staff record) to their eID data. Finally, processing is undertaken by the DFN CA in order to issue a smart certificate for the verified user.

The University is the entity that provides the services (membership to its facilities, including the ability to use a smart certificate) and that forms the contractual relationships with the user and the DFN. The University is also the entity that decides that membership checks will be performed through the Shibboleth infrastructure and ID checks will be performed either manually or through

eID. Therefore, the University determines the purposes and means of processing. **The University acts as a data controller.**

In case the Enrolment Service is provided by a third party, and not hosted within the University, **the third party that operates the Enrolment Service will act as a data processor** on behalf of the University.

The DFN also acts as a data processor on behalf of the University, providing PKI services under the instructions and to the users of the University.

Finally, the user is the data subject.

7.4.5.2 Create certificate with previously proven identity

In this scenario, processing is undertaken by the Shibboleth component of the University to confirm the user's membership, and, by the University's Service Desk staff to verify the user's identity and requires a certificate. The DFN CA processes data in order to issue the smart certificate for the verified user.

The University is the entity that provides the services (membership to its facilities, including the ability to use a smart certificate) and that forms the contractual relationships with the user and the DFN. The University is also the entity that requires the verification checks of IDs and has staffed the Service Desk to this end. Therefore, the University determines the purposes and means of processing. **The University acts as a data controller**.

The DFN acts as a data processor on behalf of the University, providing PKI services under the instructions and to the users of the University.

Finally, the user is the data subject.

7.4.5.3 Certificate management

The front-end of the service provides management capabilities to the users, including a list of issued certificates (access), the ability to back-up a certificate, the ability to download a certificate (access and portability) and the ability to revoke a certificate (objection, restriction, erasure). Not including back-up options, the management capabilities do not constitute additional processing but tools for the data subjects to exercise their rights.

Additional processing is introduced with the optional storage of certificates in an encrypted data store, where the purpose is the preservation of the certificate by the University, who is the data controller, and it will be based on user consent.

7.4.5.1 Auditing

Audit logs are created by the Enrolment Service. Insofar as the Enrolment Service is not integrated into the University's infrastructure and is operated by a third party, **the operator of the Service is a data processor** on behalf of the University. The University, for the reasons listed above, is the data controller and the principal entity with an accountability obligation. However, the timestamped logs created at the Service also fulfil the accountability obligations of the processor.

7.4.6 Data Protection by Design in the Smart Certificate pilot

The Smart Certificate pilot will be processing three sets of personal data: authentication data for the University members, identification data contained in their eID means or supplied by the Service Desk, and e-mail addresses and phone numbers for these users.

The **purpose is limited** to processing in order to issue a smart certificate to a member of the University. The **legal basis** for the pilot will likely be based on performance of a contract. Criteria for eligibility are a valid membership to the University and verification of the user's identity. Users that hold an eID means can use eID verification, whereas users without an eID means or that are unable to use their eID means can have the ID checks performed by University staff. Therefore, the pilot adheres to the principle of **fairness**. The **accountability** principle of Article 5(2) is complied with through this report focusing on the pilot along with the privacy assessments performed by the University internally about their infrastructure, and by the detailed logs for auditing purposes.

The **confidentiality** of processed data is ensured through cryptography. End-to-end encryption is set up between the FutureTrust components, the Enrolment Service and the University infrastructure. The use of the service and the FutureTrust services is secured through access control and confidentiality is further assured through mutual authentication between the components. In regards to auditing, access to the audit logs is permitted only to administrators of the system after smartcard authentication. The servers where the audit logs are held are certified through ISO 27001 standard.

The **accuracy** and **integrity** controls set up in the IdMS (through SkIDentity) are supplemented by the security policies set up at the University and the DFN and the prevention of public access to the admin interface of the service.

No particular risks to **availability** exist since the Enrolment Service does not permanently store personal data. For the same reason, the **storage limitation** principle should be considered adhered to. If the user opts to store the issued certificate, storage is protected by encryption. For the purposes of the pilot an automated clean-up process will be set up, whereby any audit logs will be deleted after successful termination of the pilot unless alternative arrangements (provided adequate controls continue to exist) are set up in communication with the participating univerisities.

The stateless operation of the Enrolment Service supports **data minimisation**. Aside from minimising the data requested to the minimum dataset determined by eIDAS, the Enrolment Service additionally performs selective disclosure of the received data: Upon receiving a username, name and email address from the University ID through Shibboleth, the Service checks only the name within the minimum dataset. If the names are sufficient for a unique match, no further processing is performed. If multiple records exist under the same name, then the Service uses the additional attributes of the minimum dataset (date of birth and address) to perform a correct match. Aside from the **unlinkability** controls implemented in the IdMS, a separation between the Enrolment Service, the Certificate Backup Storage and the Shibboleth infrastructure is implemented as an additional control.

Transparency is served through the privacy notice that details the processing, data flows and rights of the data subjects. Manual processes exist in the Service's front-end to allow the data subjects to exercise their rights (**intervenability**).

The table below maps the control measures to the feared events associated with the e-Apostille demonstrator. More specifically it describes the potential feared events that, if occurred, would impact the rights and freedoms of the data subjects, the control measures that have been introduced to mitigate the feared events and the residual risk (the likelihood of the feared event taking place *x* the severity of its impact after application of the control measures).

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
Unnecessary or unspecified processing (purpose limitation)	Limited	Specified, explicit, legitimate purposes; policies; staff training	Low
Processing not based on a lawful basis (legal basis)	Limited	Legal ground set in policy; staff training	Low
Discriminatory processing (fairness)	Significant	Supported eIDs through country profiles; all eligible students and staff of participating universities can participate	Low
Incomplete or nonexistent evidence of processing (accountability)	Limited	DPbD report; DPIA	Low
Excessive processing of data (data minimisation)	Limited	(*see* purpose limitation and unlinkability); pseudonymisation; stateless operation; no excessive data other than specified by Certification authority and Universities	Low
Processing for longer than necessary (storage limitation)	Limited	Stateless operation; deletion of data after data subject request	Low
Illegitimate access to	Significant	SSL/TLS certificates; access control;	Low

Feared event	*Level of severity/likelihood*	*Control measure*	*Residual risk*
personal data (confidentiality)			
Unwanted modification of personal data (accuracy and integrity)	Significant	SSL/TLS certificates;	Low
Disappearance of personal data (availability)	Significant	End-to-end encryption;	Low
Unnecessary linkability of attributes and/or uses (unlinkability)	Limited	Pseudonymisation; separation of domains	Low
Opaque or vague information on processing (transparency)	Limited	Context specific privacy notice of pilot	Low
Difficult or impossible exercise of data subject rights (intervenability)	Negligible	Processes to exercise data subject rights	Low

The pilotonly processes the identification data necessary to match a university member to an ID. Storage of issued certificates is optional. Therefore, by default the pilotadheres to the principles of **necessity** and **proportionality**.

8. Conclusion

This report offers a data protection risk assessment of the services developed by the FutureTrust project, as well as of the planned pilots and demonstrators, following a data protection by design approach.

In section 6 of the report, each FutureTrust service has been examined separately. First, a description of each service is conducted with an examination of each service's components, of the types of personal data processed by each service and the (personal) data flows between service components. Second, an analysis of the data protection roles and potential processing purposes and legal bases based on selected use cases is added. Third, a preliminary risk assessment is performed, which enables us to identify a preliminary list of control measures for each FutureTrust service.

	Personal data processed
IdMS	- Authentication data - Identification data o Minimum Dataset (eIDAS)

SigS	- Authentication data
	- Electronic signatures and seals
	- Electronic certificates
	  * Personal data contained in electronic documents (exceptional)
	  o Sensitive data (exceptional)

ValS	- Electronic signatures and timestamps - Authentication tokens * Personal data contained in electronic documents (exceptionally if signature object cannot be extracted)
gTSL	- Authentication data (admin group only) - E-mail addresses (for notifications; after consent)
PresS	- Authentication data - Electronic signatures and seals

Table 10: Categories of personal data processed by FutureTrust services

Based on this assessment of the services, the following observations can be made as regards the engineering of data protection principles within the FutureTrust services:

- The majority of processing of personal data by FutureTrust services concerns common personal data (see Table 10). The most common category is authentication data (username and password or authentication attestations from eID providers). The IdMS also processes identification data. Where identification data are used within the eIDAS framework, the identification data will consist of the Minimum Dataset. The SigS, the ValS and the PresS process in addition electronic signatures, seals and timestamps and associated electronic certificates. The gTSL only processes e-mail addresses of the users that opt in to the notification feature.
- On occasion, some FutureTrust services might process additional personal data. This might happen in the case of the SigS and the ValS in exceptional circumstances where electronic signatures objects cannot be extracted and parsing of the accompanying electronic document is needed. In these cases, there is a possibility that data contained in a document might belong to the category of sensitive data within the meaning of GDPR Article 9. However, no FutureTrust service is storing said documents or the data contained within.
- All personal data are confidential, secured by disk encryption, access control and secure communications (TLS encryption of the communication channels).
- All services validate the integrity of the data, either through the validation of hash values, or through checks with authoritative sources. Where necessary, logging functions have been implemented to assist in auditing the integrity of the data.
- Where additional processing is needed in order to offer added functionalities (such as, for example, the notification feature of the gTSL), the added functionality is offered as an opt in after valid consent.
- Where services can perform their purpose without the need of external datasets, the ability to function in a standalone mode keeps linkability of datasets to a minimum (see, for example, the 'application-centric signing' of the SigS).
- Finally, data minimisation is ensured in all services. Where possible services operate in a stateless mode, where no personal data are stored (Identity Broker in the IdMS, 'pop' operation in the PresS). Where possible, stored data are undergoing pseudonymisation. This happens, for example, for the FIDO authentication data in the IdMS, as well as data held by the SigS, the ValS and the PresS by replacement with hash values.
- When personal data are stored, either decentralised storage (it is the case, for example, in the gTSL Mongo DB or in the IdMS FIDO server) or storage in the control of the user is possible, depending on the implementation.

Table 11 sums up the list of controls per FutureTrust service.

Control measures	***IdMS***	***SigS***	***ValS***	***gTSL***	***PresS***
TLS	. ✓	. ✓	✓	✓	✓
Disk encryption	✓	✓	✓	✓	✓
Stateless operation	✓	--	✓	✓	✓

Control measures	***IdMS***	***SigS***	***ValS***	***gTSL***	***PresS***
User-centric storage	✓	✓	✓	--	✓
Access control	✓	✓	✓	✓	✓
Two-factor authentication	✓	--	--	--	--
Session tokens	✓	✓	✓	✓	✓
Validation of hashed data	--	--	✓	--	--
Data hashing	--	✓	✓	--	✓
Pseudonymisation	✓	✓	✓	--	✓
'Encrypt-then-sign'	--	--	✓	--	--
'Time-lock-encryption'	--	--	--	--	✓

Table 11: Data Protection by Design controls per FutureTrust services

Since the services designed by the FutureTrust project are not meant to act as standalone systems, but rather to interface with and be integrated in other eID and trust services, section 7 assesses the data protection risks when the services are integrated in the planned pilots and demonstrators. The pilots and demonstrators represent use case scenarios where FutureTrust can add value to existing or innovative services by providing access to eID and Trust Services.

Section 7 offers a description for each pilot and demonstrator. It then details the personal data processed by each, along with the processing purposes and the legal bases most likely to be suitable for the processing. Details of the data flows between the FutureTrust services and their integration environment are given next, followed by an analysis of the data protection roles. Finally, a risk assessment is performed, which enables us to identify the list of control measures and highlight the data protection level that can be achieved by each pilot and demonstrator.

Personal data processed

eInvoice	- Identification data of the company representative - Electronic signature
e-Mandates	- Authentication data to the service provider - Authentication data to the bank - Personal data within the e-Mandate
e-Apostille	- Authentication data to the service provider - Personal data within the e-Apostille
Smart Certificates	- Authentication data for the University - Identification data (minimum dataset) - E-mail address

- Phone number - Electronic signature

Table 12: Personal data processed by the pilots and demonstrators

The following observations can be made in regard to the pilots and demonstrators:

- The majority of pilots and demonstrators process only authentication data (login credentials), email addresses and electronic signatures.
- Occasionally, additional personal data might be processed, where such data are contained within submitted documents (electronic mandates and electronic apostilles). However, for the purposes of the pilots and demonstrators, none of these data are forecasted to be sensitive personal data, in the meaning of Article 9. Obviously, in a production environment additional checks should be introduced if documents with sensitive data are expected.
- Where processing for additional services is necessary (e.g. to preserve validations), this processing is an opt in based on user consent.
- The participation in the pilots and demonstrators requires only possession of a supported eID means or supported trust service (electronic signature). Although support for most formats is included by default, additional formats can be added through a templating engine. Therefore, no discrimination during the processing is expected.
- All pilots and demonstrator process the data strictly necessary to perform their processing purpose. Where less data than those contained within the minimum datasets of eIDAS (which is the default received dataset) are required, the FutureTrust services selective disclose the necessary attributes to the pilots and demonstrators.
- Most services within the pilots and demonstrators operate in a stateless manner, without permanently storing received personal data. Data storage happens only when necessary, or after user consent, and is accompanied with appropriate data subject rights management.
- All communication between the pilots' services uses encryption and access management. Therefore, confidentiality of data in transit is ensured. Confidentiality of data at rest is established through disk encryption. The end-to-end encryption, along with backup options, also ensures the availability of data.
- The accuracy and integrity of data are maintained through certificates and detailed audit trails.
- Several safeguards are in place to ensure adequate unlinkability of data, from separation of domains and entities to pseudonymisation and hashing.
- Finally, all pilots and demonstrators have automated, semi-automated or manual processes to allow data subjects to exercise their rights throughout their operation. For the pilots and demonstrators that will not progress to a production environment after the end of the project, all processed personal data will be automatically deleted.

Table 13 sums up the residual data protection risk per goal after safeguards and controls were put in place.

Data protection goal	***eInvoice***	***e-Mandates***	***e-Apostille***	***Smart Certificate***
Purpose limitation	Low	Low	Low	Low
Legal basis	Low	Low	Low	Low
Fairness	Low	Low	Low	Low
Accountability	Low	Low	Low	Low
Data minimisation	Low	Low	Low	Low
Storage limitation	Low	Low	Low	Low
Confidentiality	Low	Low	Low	Low
Accuracy and integrity	Low	Low	Low	Low
Availability	Low	Low	Low	Low
Unlinkability	Low	Low	Low	Low
Transparency	Low	Low	Low	Low
Intervenability	Low	Low	Low	Low

Table 13: Residual risk for the pilots and demonstrators

It should be noted that the assessments presented in this document are not meant to replace a DPIA within the meaning of GDPR Article 35. It is instead a necessary step to assess the data protection by design afforded by the FutureTrust services and pilots and form a primer on which a future DPIA can be based on, if the piloted services move to a production environment.

However, for the purposes of the FutureTrust project, it can be asserted that the FutureTrust services have been engineered to offer 'by design' and 'by default' control measures for all data protection goals. This is demonstrated in the assessment of the three types of feared events during the assessment of the FutureTrust services but also in the assessment of all data protection goals when the services are integrated into an operational environment within a pilot or demonstrator. The processing of personal data taking place in the context of these services is necessary to pursue the potential purposes examined and the advantages derived from the use of these services as designed are not outweighed by disadvantages or negative impacts upon data subjects' rights on the basis of the use cases described. As aforementioned, the controls aimed at the FutureTrust services should be supplemented by further organisational and technical measures when the services are integrated into different environments and a DPIA should be performed.

Nonetheless, this data protection by design assessment demonstrates that the FutureTrust services have been designed to adhere to the obligations set forth by the GDPR and support a high level of data protection by design. It is hoped that adoption of the FutureTrust services by service providers will encourage the use of GDPR compliant Trust Services and will assist data controllers in meeting their obligation under the GDPR.

9. References

Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, adopted on 16 February 2010)

Bieker F and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' in Schiffner S and others (eds), *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings* (Springer International Publishing 2016)

Bouckaert V and others, D3.3 - Comprehensive Validation Service (final v 1,00, FutureTrust project, 30 May, 2017)

Bygrave LA, 'Hardwiring Privacy' in Brownsword R and others (eds), *The Oxford Handbook of the Law and Regulation of Technology* (Oxford University Press 2017)

Cardoso C and others, D3.7.4 - SEPA e-Mandates Demonstrator (v10, 16 May 2017)

Chalupar A, D4.6 - Identity Management Service (draft v 0,03, FutureTrust project, 10 July, 2018)

CNIL, Privacy Impact Assessment (PIA): Knowledge Bases (edition of February, 2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> accessed 25 May 2018

--, Privacy Impact Assessment (PIA): Methodology (edition of February, 2018) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf> accessed 25 May 2018

Conference of the Independent Data Protection Authorities of eh Bund and the Länder, The Standard Data Protection Model (V1,0 - trial version, March, 2017)

Elliot M and others, *The Anonymisation Decision-Making Framework* (UKAN 2016)

Hühnlein D and others, D3.6 Remote Signing and Sealing (Design Documentation, v1,0, FutureTrust project, 31 May, 2017)

Hühnlein D and others, D3.5 Identity Management Service (Design Documentation, v 1,0, FutureTrust project, 30 May, 2017)

ICO, Data Protection Impact Assessments (DPIAs) (The General Data Protection Regulation: Accountability and Governance, 22 March, 2018) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf> accessed 25 May 2018

--, Guide to the General Data Protection Regulation (1,0,154, 4 June, 2018) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 24 May 2018

Karsch C, D4.10 German Pilot (Design Documentation, v 1,0, FutureTrust project, 22 June 2019)

Opinion of Advocate General Bot on 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, EU:C:2017:796

Piswanger C-M and others, D3.7.1 - eInvoice submission to the Austrian Public Sector using web service authentication and eSignature (AT pilot and demonstrator) (v11, 31 May 2017)

Piswanger C-M and Zehetner C, D4.9 - Austrian Pilot Service Implementation Documentation (v11, 28 February 2019)

Prechtl M, Hühnlein D and Kühne A, D3.4 - Scalable Preservation Service (final v 1,0, FutureTrust project, 31 May, 2017)

Spiekermann S and Cranor LF, 'Engineering Privacy' (2009) 35 IEEE Transactions on Software Engineering 67

Tsakalakis N and Stalla-Bourdillon S, D2.8 - Documentation of the Legal Foundations of Trust and Trustworthiness (FutureTrust project, v 1,00, 29 June, 2018)

Wiese Schartum D, 'Making privacy by design operative' (2016) 24 International Journal of Law and Information Technology 151