TOOP Trust Architecture

Luca Boldrin[1], Giovanni Paolo Sellitto[2](✉), and Jaak Tepandi[3]

[1] InfoCert, Rome, Italy
luca.boldrin@infocert.it
[2] ANAC, Rome, Italy
g.sellitto@anticorruzione.it
[3] Information Systems Group, Tallinn University of Technology, Tallinn, Estonia
jaak.tepandi@taltech.ee

Abstract. While information security nowadays represents a core concern for any organization, Trust Management is usually less elaborated and is only important when two or more organizations cooperate towards a common objective. The overall Once-Only Principle Project (TOOP) architecture relies on the concept of trusted sources of information and on the existence of a secure exchange channel between the Data Providers and the Data Consumers in this interaction framework. Trust and information security are two cross-cutting concerns of paramount importance. These two concerns are overlapping, but not identical and they span all of the interoperability layers, from the legal down to the technical, passing through organizational and semantic layers. While information security aims at the preservation of confidentiality, integrity and availability of information, trust establishment guarantees that the origin and the destination of the data and documents are authentic (authenticity) and trustworthy (trustworthiness), and that data and documents are secured against any modification by untrusted parties (integrity). In this chapter, the TOOP Trust Architecture is presented, starting from a simple abstract model of interaction between two agents down to the detailed end-to-end trust establishment architecture, modeled onto the Toop Reference Architecture presented in the previous chapter.

Keywords: Security · Trust · Enterprise Architecture

1 Introduction

In the logic of the "once only principle" there is one single entity which is entitled to provide evidence in support of a specific claim, therefore TOOP significantly relies upon trusted and managed sources of information, which in many cases are also called Base Registries. 'Base registry' refers to a trusted and authentic source of information under the control of a public administration or of an organisation entitled by a law provision. According to the European Interoperability Framework 2.0, base registries are 'reliable sources of basic information on items such as persons, companies, vehicles, licences, buildings, locations and roads' and are 'authentic and authoritative, and form, separately or in combination, the cornerstone of public services' [6]. In the context

R. Krimmer et al. (Eds.): The Once-Only Principle, LNCS 12621, pp. 126–140, 2021.
https://doi.org/10.1007/978-3-030-79851-2_7

of a cross-border architecture, spanning different policy domains, it is of paramount importance to guarantee trust establishment between the parties that interact to provide the Once-Only Principle (OOP) service. Therefore trust establishment complements the usual information security management concerns. Information security and trust establishment represent two overlapping, but not identical concerns and they span all of the interoperability layers, from the legal down to the technical, passing through organizational and semantic layers.

The standard ISO/IEC 27000:2018 [1] defines information security as preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, trustworthiness, accountability, non-repudiation, traceability, and reliability can be involved. Trust establishment guarantees that the origin and the destination of the data and documents are authentic (authenticity) and trustworthy (trustworthiness), while security ensures that data and documents are protected against any modification by untrusted parties (integrity) [2–4]. The implementation of trust relies on the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereafter the eIDAS Regulation).

As an example of the differences between the concepts of security and trust, security usually does not involve trustworthiness of the data origin (this is not the same as authenticity - property that an entity is what it claims to be). On the other side, trust usually does not involve availability, reliability, and all aspects of confidentiality. Additional constituents of trust management - accountability, non-repudiation, traceability, and confidentiality[1] can be supported by maintaining processing logs and other controls, encrypting data and documents during the transmission, etc. In general, a Security Architecture involves the general approach to security and controls not directly related to trust, while Trust Architecture includes controls and procedures associated with establishment of trust. Privacy, which is one of the main concerns when handling pieces of information about natural personae, can be handled in the context of trust and security, introducing the concept of consent. In addition, trust requires a clear definition of roles and reliable identities of the entities assigned to those roles.

The Trust Architecture as devised in the TOOP Reference Architecture focuses on the trust establishment between the actors involved in an OOP System to provide guarantees on the origin, destination, authenticity (property that the entity providing the data is what it claims to be), trustworthiness (property that the entity providing the data can be relied on as honest or truthful), and integrity of information that is exchanged between the actors. This architecture makes a distinction between the TOOP specific and non-specific requirements, trust relationships, and controls related to trust establishment.

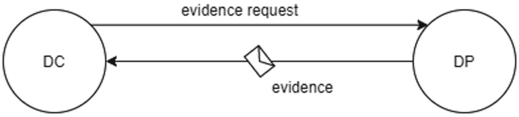
The rest of this Chapter is structured as follows: in Sect. 2 we present an overview of the trust concept and related literature. In Sect. 3 an overview of solutions for establishing trust is presented. The more specific TOOP requirements and solutions are discussed in Sect. 4, which introduces the concept of End-to-End Trust and in Sect. 5, where the TOOP reference Trust Architecture is presented. In the final Sect. 6, we draw some conclusions and discuss the points that are still open.

[1] Here Confidentiality is intended as a component of trust management not as a security related feature.

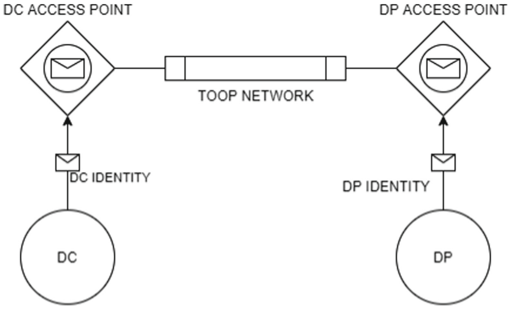
2 Overview of the Trust Concept

Trust in the digital domain has been widely addressed in the literature as a border territory between philosophy, management, law, information technology and sociology (see for example [5] for a literature review). A computational definition of trust was devised by Marsh[2], who gave a formal model for representing trust in mathematical terms.

For our purposes we take a simplified and pragmatic view, which is however consistent with ISO/IEC 27000-series and aligned with the "trust service" concept introduced by EU Regulation [eIDAS]. In this setting, we are dealing with two parties: a sender of data and a recipient of data.



In order to identify the actors involved in trust establishment and the pieces of information that they exchange, which in turn represent the assets to be protected, we can refer to an abstract[3] trust establishment process, considering a simple interaction model between a Data Consumer (DC) and a Data Provider (DP). Taking into account the overall architecture of the EU digital Service infrastructure that connects the Data Provider and the Data Consumer, the interaction can be abstracted as a communication through two access points and therefore we must consider the exchange of information between DP/DC and their respective access points (APs), where the information is the DP/DC identity, the source is respectively DP/DC and the consumer is the Access Point (AP) that must identify DP/DC.



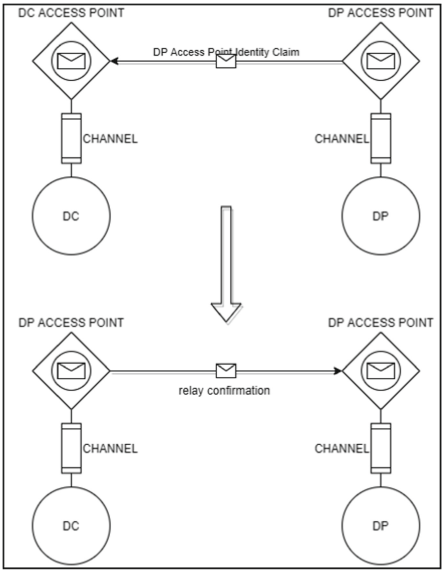
Once the DP and DC have been recognized by their respective Access Points, the Access Points must establish a channel and the communication is between Access Points: the information exchanged is the Access Point Identity Claim and the response relay confirmation.

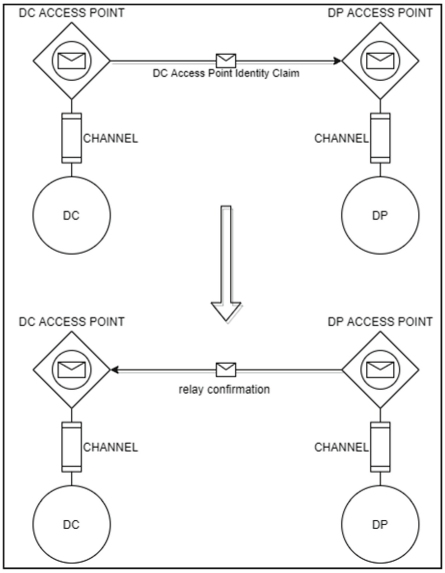
We have here that AP1 (Source) sends an AP1 Identity Claim (Information) to AP2 (Consumer), AP2 (Source) sends an AP2 Identity Claim (Information) to AP1

[2] Marsh, Stephen. 1994. "Formalising Trust as a Computational Concept".

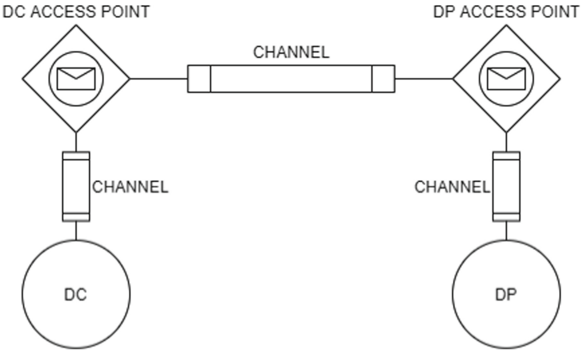
[3] In this case, the term "abstract" refers to the absence of any reference in this model to a specific technology or standard to support the trust establishment process. The technical solutions will be examined in the following paragraph.

(Consumer) and in response AP2 (Source) sends a relay confirmation (Information) to AP1(Consumer).

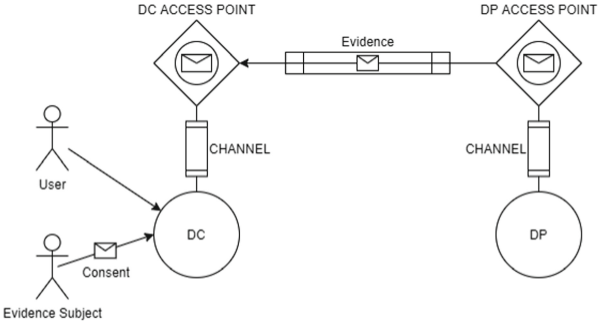




These interactions lead to the creation of a secure and trusted channel between the Data Consumer and the Data Provider: the channel will be used by these two nodes to communicate.



After the channel is established, the User (Source), which is the Data Subject or acts on behalf of the Data Subject must send the Consent (Information) to the Data Provider (Consumer). The user Consent (Information) is also sent by the Data Consumer vouching for the user (Source) to the Data Provider (Consumer) that in response, as Source, will send the DP Identity (Information) to the User (Consumer).



It is worth noting that this approach embraces the fundamental issue of "identification of the sender" as a special case of trust establishment. In this case, the original trust question specifies: "how can the recipient assume that the sender is the one he/she claims to be?". The data provided by the sender therefore consists in an "identity claim" i.e., a set of attributes which allows the recipient to have a partial/total knowledge on the real world identity of the sender. The trust establishment process supports the recipient in validating that data, therefore acquiring some confidence on the identity of the sender.

3 Solutions to Establish Trust

The basic trust establishment process is presented here in an abstract and simplified manner, without referencing any specific organizational, legal or technical solution or standard. It is essentially an organizational process, which shall be supported by technical (digital in the XXI century) solutions to establish and maintain security and trust. In the case of the exchange of an evidence from DP to DC, DC needs to trust the evidence provided by DP. While this is certainly an over-simplification, the main approaches to the establishment of digital trust[4] fall into the following classes:

- ***trust by history***: the data is assumed to be true because it comes from a sender which proved honest in previous interactions. This method implies that the recipient has the means to identify the sender through multiple transactions.
- ***trust by reputation***: the data is assumed to be true because the sender's trustworthiness is vouched for by other actors. This method implies that there is a reliable way to collect feedback by (possibly many) other parties.
- ***trust by liability***: the data is assumed to be true because there is a way of enforcing liability on the provided data. This method implies the knowledge of the real-world identity of the issuer of the data (which may differ from the sender) as well as a way to verify who is entitled to provide some type of data (a criminal record certificate can only be attested by the appropriate law enforcement agency).

The main concern of the TOOP Trust Architecture is to ensure that any sociotechnical system compliant with TOOP Reference Architecture (TOOPRA), in addition to the

[4] For a deeper analysis see Luhmann, Niklas. 2000. Familiarity, Confidence, Trust: Problems and Alternatives.

main concern (the Once only Principle), will also preserve trust and the related security features, by default and by design. Ensuring trust by design entails a well-thought mix of the three approaches to guarantee that trust will be preserved over the entire lifecycle of the TOOPRA compliant socio-technical system.

The scenario addressed by TOOPRA can involve organizations that could have had no previous interaction, therefore the preferred choice is trust by liability, possibly in conjunction with trust by reputation, which makes it possible to assume trust in some well-known data providers established or appointed as the trustable data sources by law (a Ministry, etc.). Controls related to trust management not specific to TOOPRA must still be implemented.

Additionally, most of the trust scenarios managed in TOOP rely on trust by liability, supported by some existing general purpose trust-enabling tools:

- **electronic identity (eID)**: this term identifies the digital identities provided by national electronic identity systems which are mutually recognized across EU countries by virtue of eIDAS Regulation [eIDAS] and the associated Implementation Acts (IA 1501/2015, IA 1502/2015, IA 1984/2015]. The eID building block also comprises the technological infrastructure which has been set up in order to support cross-border electronic identity interoperability (the so called “eIDAS network”).
- **electronic delivery (eDelivery)**: this term identifies “a service that makes it possible to transmit data between parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations” [eIDAS art 3 (33)]. Such services are offered by third parties in compliance with eIDAS regulation on Trust Service Providers, and provide legal value as established in [eIDAS art. 43, 44].
- **electronic signature/seal (eSignature/eSeal)**: this term identifies the tools and services to support non-repudiability of data, based on “certificates” issued by a Certification Authority.

These services are provided by Trust Service Providers, and provide legal value as established in [eIDAS art. 25, 35]. While the regulation is technologically neutral, public administrations are bound to accept specific formats for signatures[5], which are defined by the European Telecommunications Standards Institute (ETSI)[6] in the following specifications, namely the baseline specification for Advanced Electronic Signature

[5] Ruled by the Commission implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1506.

[6] ETSI is an independent, not-for-profit, standardization organization in the information and communications technology industry fulfilling European and global market needs. ETSI supports the development and testing of standards for ICT-enabled systems, applications and services.

of XML[7], CMS[8] and PDF[9] documents and a specification for a digital Container[10], to bind together one or more signed objects with their advanced electronic signatures or time-stamp tokens.

Electronic delivery services (e-Delivery Building Block) are not bound to specific technological implementations. TOOP adopts as much as possible the building blocks provided by the Connecting Europe Facility (CEF) Digital Service Infrastructure (DSI), specifically:

– CEF eSignature building block[11], which provides off-the-shelf components to implement eIDAS compliant advanced/qualified digital signature.
– CEF eID Building Block[12], granting cross-border authentication for TOOP-enabled services through national eIDAS Nodes.
– CEF eDelivery[13] building block, which allows to create a network of nodes for secure digital data exchange and the creation of a safe and interoperable channel to transfer documents and data between organizations ensuring data integrity and confidentiality in every transmission through the use of digital signatures and encryption.

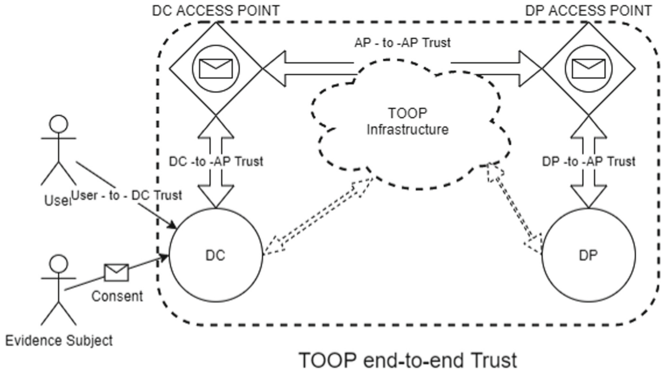
These Building Blocks enable legal assurance and accountability in the exchange of data and documents. As an example, eDelivery mandates that the recipient of a message must send a digitally signed acknowledgement of receipt for every message received.

4 Establishing the End-to-End Trust

The overall Trust and Security architecture of TOOP relies heavily on a set of building blocks which ensure, in the technology layer, the possibility to create a distributed network of trusted partners. This particular architecture enables a community-based approach to digital trust, based on the existence of a network of trusted nodes (Access Points), which provide the capability to establish a secure and trusted channel between different public and private organizations. The Technology layer is complemented by the Organizational layer and the Legal layer, where the governance model is specified respectively in terms of Business Interoperability specifications, which are agreements between the organizations participating in the community, and with regulations or laws that establish the Owners of the Trusted Data Sources, i.e. the organizations in charge of the governance of the Base Registries.

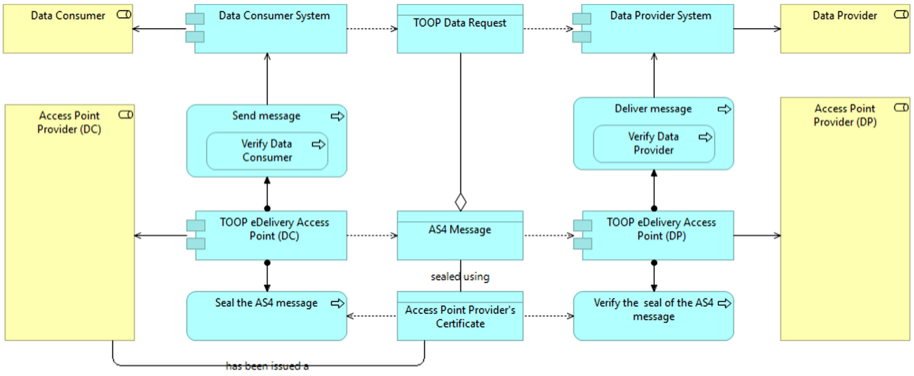
The resulting end-to-end trust view between the DP and DC is specific to the OOP Reference Architecture (TOOPRA). It is depicted on the following diagram, involving the Data Consumer (Competent Authority acting as a Data Consumer) certificate used for sealing the TOOP Data Request.

[7] XML Advanced Electronic Signature (XAdES), specification ETSI TS 103171.
[8] PDF Advanced Electronic SignaturePAdES - ETSI TS 103172.
[9] CMS Advanced Electronic Signature CAdES - ETSI TS 103173.
[10] Associate Signature Container (ASiC) Baseline Profile - ETSI TS 103174.
[11] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature.
[12] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID.
[13] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery.



In addition to the TOOPRA specific trust relationships, an OOP system involves trust relationships not specific to TOOPRA. For example, trusting the Data Consumer to Access Point and Access Point to Data Provider communications, Routing Metadata Discovery data, eIDAS Node data, DNS Server data, AS4 Message Service data, and Central Trust List server data is not dependent on TOOPRA. These relationships are represented in the TOOP Reference Architecture diagrams by pointing to a (cloud) TOOP infrastructure, nevertheless they must be trusted by the stakeholders.

The brokered trust through the Access Point gateways is depicted on the following diagram. It relies on the use of the Access Point Provider certificates from both the Data Provider and the Data Consumer Member States and involves verification of the Data Provider and Data Consumer, sealing the AS4 Message using the Access Point Provider certificate, as well as verification of the seal of the AS4 Message.



All the assets identified above, as well as the relationships (communications involving data belonging to these assets), need to be trusted.

Trusting the Assets

In trusting the assets, the main emphasis is on the authenticity and trustworthiness of the data sources, as well as integrity of data processing within the stakeholders, e.g., data owners, maintaining the assets.

The user identification and authentication data, request data, and consent data are created during the evidence exchange between the Data Consumer and the Data Provider.

The mechanisms for trusting both these assets and their relationships must be provided. Quality of other information assets involved in TOOPRA is the responsibility of the respective data owners and thus outside the TOOPRA scope; this applies also to the authenticity and trustworthiness aspects of data assets. Thus in TOOPRA only mechanisms for trusting the relationships between these assets are provided.

Trusting the Relationships

In trusting the relationships, the main emphasis is on the integrity of data - the stakeholders need to be sure that the assets have not been modified by untrusted parties.

The following table presents a list of main TOOPRA specific trust relationships. The trust establishment relies significantly on the eIDAS Regulation. Taking into account the potentially critical nature of transactions, the general requirement is that the trust services are qualified. Special cases need to be considered on a case by case basis.

Table 1. List of main TOOPRA specific trust relationships

Information asset (data)	Source	Destination
User request to retrieve evidence User consent	User	Data consumer
User identity User consent between DC and DP Evidence Request from DC to DP Evidence retrieved from DP Evidence processed by DP Evidence provided to DC	Data provider/data consumer	Data consumer/data provider
The user identification and authentication	User	Data consumer
DP discovery data, data services directory Identification of public organisations	Data consumer/data services directory	Data services directory/data consumer
Data from the criteria and evidence type rule base required evidence identification data	Data consumer/criteria and evidence type rule base	Criteria and evidence type rule base/data consumer
Semantic mediation data	Data consumer/ontology repository	Ontology repository/data consumer

For all of the information assets exchanged in the interactions reported in Table 1, the trust establishment solutions usually comprise trust services (e.g., qualified electronic signatures, qualified electronic registered delivery services, qualified electronic seals, or transactions secured by qualified certificates for website authentication) according to the eIDAS Regulation as mechanisms that ensure secure and protected data exchange in public services. In addition, we can provide other relevant general and TOOP specific trust and integrity related controls indicated in the next section.

5 The TOOPRA Trust Architecture

Trust establishment guarantees that the origin and the destination of the data and documents are authentic and trustworthy, and that data and documents are secured against any modification by untrusted parties. Trust management can also involve authorization, accountability, non-repudiation, traceability, as well as confidentiality as a component of trust management.

The preceding sections have detailed the methods to set up a secure and trusted channel between a DP and a DC. Based on these considerations, the current section presents the steps needed to establish trust.

From the architecture development point of view, the TOOP security and trust architectures have been designed adopting the ISO/IEC 27000-series of standards. The overview standard of this series, ISO/IEC 27000:2018, proposes the notion of an Information Security Management System (ISMS), consisting of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization to protect its information assets.

The following steps are needed to establish, monitor, maintain, and improve an ISMS:

- identify information assets;
- identify associated information security requirements;
- assess and treat information security risks;
- select and implement relevant controls to manage unacceptable risks;
- manage the ISMS - in particular, monitor, maintain and improve its effectiveness.

These steps are detailed below.

Assets

The trust architecture is developed based on information assets subject to trust management. All these assets need to be trusted - for example, the stakeholders need to be sure that the assets have not been modified by untrusted parties.

Based on the Business Architecture, Information System Architecture, and Technology Architecture views, the following information assets are identified.

Various data related to the users must be trusted, such as the User identification and authentication data, the User identity data, the User request data to retrieve evidence, and the User consent data.

To find data providers and retrieve evidence, the data from the Criteria and Evidence Type Rule Base, the required evidence identification data, the data on the request for evidence from DC to DP, the Data Provider Discovery data, data from the Data Services Directory, the identification data of Public Organisations, and the semantic mediation data need to be trusted as well.

Various other kinds of data, such as data about the User consent exchanged between the DC and DP, data of the evidence retrieved from the Data Provider, data of processing the evidence retrieved from the Data Provider, data of the evidence provided to the Data Consumer, and the evidence exchange data are needed and must be trusted.

Finally, various kinds of technical data must be trusted to provide an OOP service: routing Metadata Discovery data, including data in the SMP and BDXL, eIDAS Node data, DNS Server data, and AS4 Message Service data.

Requirements

The following TOOP specific requirements related to trust establishment have been reported.

- The authenticity of the data transmitted by the DP must be trusted by the DC
- The transmission of an Evidence from DP to DC must guarantee the integrity of the exchanged Evidence
- The Data Provider is responsible for transmitting the requested Evidence in accordance with the confidentiality and integrity requirements
- Any exchange of evidence organised under the OOP must be possible to verify by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the time of the exchange, and the integrity/authenticity of the exchanged data itself)
- The technical system shall in particular ensure the confidentiality and integrity of the evidence
- A common security and privacy framework must be defined and processes for public services must be established to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses
- Trust services must be used according to the Regulation on eID and Trust Services as mechanisms that ensure secure and protected data exchange in public services
- A level of security appropriate to the risk, including inter alia as appropriate the ability to ensure the ongoing integrity of processing systems and services, must be ensured by the competent authorities and any other participants in the evidence exchange mechanism
- The user must have the possibility to preview the evidence to be used by the DC, and check the validity of the retrieved information

Risks

Assessment and treating of specific trust related risks deals with the authenticity and trustworthiness aspects of creating and exchanging data.

All the assets identified above, as well as the relationships (communications involving data belonging to these assets), need to be trusted. In trusting the assets, the main emphasis is on the authenticity and trustworthiness of the data sources, as well as integrity of data processing within the stakeholders, e.g., data owners, maintaining the assets.

The user identification and authentication data, request data, and consent data are created during the evidence exchange between the Data Consumer and the Data Provider.

Quality of other information assets involved in TOOPRA is the responsibility of the respective data owners and thus outside the TOOPRA scope.

The highest trust related risks concern data of the evidence (data in transit) in Single Digital Gateway Regulation (SDGR) domain: data related to both citizens and businesses as stated in the SDGR.

Also significant are risks related to the data of the evidence (data in transit) in TOOP domain: information related to business activities and on cross-border sharing of this information.

The User request data, response data, consent data, activity log data need to be trusted as well. Integrity of information assets related to central services and components: the Criterion & Evidence Type Rule Base, Data Services Directory, Ontology Repository, SMP, BDXL must be preserved.

A risk treatment decision must be made with respect to all risks. The stakeholders should establish criteria for determining which risks can be accepted. Options for risk treatment include applying controls to reduce the risks, accepting the risks that satisfy the criteria for risk acceptance, avoiding risks, as well as sharing the risks to other parties, for example to insurers or suppliers. These options depend on the legislation and organisational policies of particular information system stakeholders. Therefore they must be further specified in the system initialization and development processes.

Controls

Establishment of trust depends both on the assets and communications created specifically for a TOOPRA based system, as well as on supporting assets and communications that exist independently of such a system. The following organisational and technical controls must be taken into account to ensure appropriate level of trust related to both TOOPRA specific and non-specific components and relationships, independently of who implements them:

- use of trust services according to the eIDAS Regulation as mechanisms that ensure secure and protected data exchange in public services;
- ensuring that the competent authorities and any other participants in the evidence exchange mechanism implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate the ability to ensure the ongoing integrity of processing systems and services;
- ensuring that all the information assets identified in the above sections can be trusted.

The relevant general trust and integrity related controls include as appropriate classification of information in terms of integrity, usage of public key cryptography and digital signatures, issuing public key certificates by a recognized certification authority, appropriate handling of public and private keys, suitable authentication processes, using trusted third parties to provide application services, segregation of networks based on trust levels, ensuring trustworthiness of personnel working with the system, use of cryptographic techniques to protect integrity and authenticity of information, providing protection from malware, providing adequate backup facilities, establishing network controls to safeguard integrity of data passing over public networks or over wireless networks, applying appropriate logging and monitoring to enable recording and detection of actions that may affect information security, enforcing formal change control procedures to ensure the integrity of systems, applications and data, introducing incident response measures related to loss of integrity, and other.

A process must be introduced for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The technical controls must ensure that the authenticity of the data transmitted by the DP is trusted by the DC, that the transmission of an evidence from DP to DC will guarantee the integrity of the exchanged evidence, and that the Data Provider acknowledges the responsibility for transmitting the requested evidence in accordance with the confidentiality and integrity requirements.

The following building blocks, standards and interfaces need to be supported to achieve the appropriate trust level:

- ETSI ASiC Specifications: Electronic Signatures and Infrastructures (ESI), ASiC Baseline Profile Technical Specification and Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) Technical Specification;
- the CEF eSignature and eID Building Blocks;
- the CEF eDelivery AS4 profile for message exchange;
- the CEF eDelivery profile of the BDXL specification;
- the OASIS Service Metadata Publishing 1.0(BDXR SMP) specification;
- the CEF eIDAS Profile.

Management of the ISMS

The stakeholders of an information system based on the Once-Only Principle need to maintain and improve the ISMS. This is done by monitoring and assessing performance against organizational policies and objectives, and reporting the results to management for review. The review evaluates whether the ISMS includes specified controls that are suitable to treat risks within the ISMS scope. Based on the records of these monitored areas, it provides suggestions for corrective, preventive and improvement actions.

All TOOP specific data, as well as associated systems and communications, must be monitored. Regular testing, assessing and evaluating the effectiveness of technical and organisational measures is needed for ensuring the security of the processing.

6 Conclusion

Trust between the users, data subjects, data providers, data consumers, and other stakeholders involved in an OOP system is of vital importance. Without digital trust, the stakeholders will not use services of an OOP system.

Digital trust can be established by liability (there is a way of enforcing liability on the provided data), reputation (the sender's trustworthiness is vouched for by other actors), construction (the system is designed and developed to preserve trust), and /or history (the sender has proved honest in previous interactions). For real-life applications, all these aspects are important.

From the legal and organizational point of view, the OOP is mainly interested in the concept of trust between Organizations and the legal interoperability between different policy domains. The achievement of these two objectives is deeply rooted in the Semantic and Technical layer, where the means to ensure the semantic equivalence for the evidence that are exchanged between DP and DC and their integrity and availability must be ensured.

From a technical point of view, the establishment of trust between organizations, be them public or private, and the possibility for citizens and business to re-use some documents across different contexts, possibly cross-border (as postulated by the OOP) requires a framework for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union.

Trust by construction also assumes the chain of trust: trusted source, trusted communications, trusted intermediate nodes, and trusted processing in the nodes.

In turn, the technical framework can hold only if some organizational and legal basis for collaboration between different entities exist and if the exchanged information maintains its meaning or can gain some meaning also in a different organizational context.

The diffusion of mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities, facilitating the adoption of the OOP.

Finally, without a history of successful use of different OOP systems, the users, organisations, and governments will not trust them. The TOOP Reference Architecture gives a tool for more efficient development of such systems and for design of trust as a component in their construction.

References

1. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary
2. Cofta, P.: Trust, Complexity and Control: Confidence in a Convergent World. John Wiley I and Sons (2007)
3. Raj, G., Sarfaraz, M., Singh, D.: Survey on trust establishment in cloud computing. In: 2014 5th International Conference - Confluence the Next Generation Information Technology Summit (Confluence), pp. 215–220 (2014)
4. Winslett, M., et al.: Negotiating trust in the web. IEEE Internet Comput. **6**(6), 30–37 (2002)
5. Taddeo, M.: Defining trust and e-trust. Int. J. Technol. Hum. Interact. **5**, 23–35 (2011). https://doi.org/10.4018/jthi.2009040102
6. European Interoperability Framework 2.0