User Requirements of Trusted Third Parties in Europe[#]

Dimitrios Lekkas[+], Sokratis K. Katsikas[+], Diomidis D. Spinellis[+], Pavel Gladychev[*] and Ahmed Patel[*]

[+] *Department of Information and Communication Systems, University of the Aegean, Karlovassi GR-83200, Greece, e-mail:{dlek,ska,dspin}@aegean.gr*

[*] *CNDSRG, University College Dublin, Belfield, Dublin 4, Ireland, email: {apatel, pavel}@net-cs.ucd.ie*

Key words: Trusted Third Parties, user requirements, legal requirements

Abstract: We review the Public Key Infrastructure in Europe as outlined in various INFOSEC and ACTS projects. The objective is to specify an abstract reference model for the PKI as a combination of the results of various European projects, which is scaleable, based on standards and flexible across different domains, geographical areas and business sectors. The user requirements in various business domains, such as health, transport and public information systems are extracted and highlighted. The user needs are then used as the reference for the development of the services that a Trusted Third Party must offer to its users and consequently they will be the base for

[#] In Simone Fisher-Hübner, Gerald Quirchmayr, and Louise Yngström, editors, *User Identification & Privacy Protection: Applications in Public Administration & Electronic Commerce*, pages 229-242, Kista, Sweden, June 1999. IFIP WG 8.5 and WS 9.6.

This is a machine-readable rendering of a working paper draft that led to a publication. The publication should always be cited in preference to this draft using the reference in the previous footnote. This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

the construction of an abstract reference model. This model outlines in general terms the entities involved in the provision of TTP services and the functions supporting their interactions.

1. INTRODUCTION

The use of electronic messaging is becoming more widespread as Information and Communication Technology becomes more effective and cheaper and telecommunications become more advanced. However, the increased user interconnectivity, the growth of electronic commerce, and the reliance upon electronic communications means that more information is being carried electronically. Sensitive information such as contracts, money transactions, and personal details become vulnerable to attacks such as eavesdropping, non-authorised modification, and masquerading.

A Public Key Infrastructure — using public and private keys for data encryption and for digitally signing of messages — can play an integral role in facing these attacks by providing end-to-end security of information in terms of confidentiality, integrity, availability, and non-repudiation security services. The strength of these security services depends upon the security of the underlying keys, whether they are used for data encryption or for message signing. Security is therefore based on the protection of the confidentiality of the private keys and the integrity of the public keys in the delivery and storage processes.

In a small community, the integrity of the public keys could be ensured by manual delivery of the keys. However, in a international electronic messaging environment the manual delivery of keys between users is not adequate. Automatic key management by a trusted agent is necessary; this must be performed by a Trusted Third Party (TTP) in order to facilitate the use of public key cryptography and digital signing.

The main goal of this paper is to present a review of the TTP user requirements in various domains, notably health care, public transport, shipping, and public information systems as dealt with in several INFOSEC and ACTS projects. The basic user requirements in the aforementioned sectors proved to be similar, though the level of importance of particular requirements is different and there are some additional domain-specific requirements.

Most of the projects specified as a minimal set of security services that would serve the user requirements: the authentication of users, the integrity of messages, the privacy and confidentiality of messages, the non-repudiation of message origin and receipt, and the availability of the offered services. Additionally, the issues that have been recognised as important in some of the projects are the anonymity of participants, time-stamping, ease of use, the

uniqueness of the documents, protection of the transacting parties from abuse, and various legal issues.

The solutions offered in the examined projects, although they assert a substantial support for facing the common security threats in their specific domains, they do not provide for any inter-domain operability nor for the construction of a common reference model, based on commonly accepted standards.

This review aims to contribute to the specification of an abstract reference model for the PKI as a combination of the results of various European projects, which is scaleable, based on standards, and flexible across different domains, geographical areas, and business sectors. It combines and collates the results of earlier INFOSEC and ACTS projects, allowing the development of a common reference model and of common terminology that can be used across different business sectors and national borders. Finally, it addresses the provision of services enabling the cross-certification procedures and contributes towards the standardisation of the TTP services.

The paper is structured as follows: In section 2, the fundamentals of TTPs are briefly provided. Section 3 offers an overview of the projects that were reviewed. Section 4 presents the TTP user requirements as captured by the projects described in section 2. The same section discusses legal TTP requirements. Finally, section 5 summarises our conclusions.

2. TRUSTED THIRD PARTY FUNDAMENTALS

As described in [Castell, 1993]: *"A TTP is an impartial organisation delivering business confidence, through commercial and technical security features, to an electronic transaction. It supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means"*.

2.1 A typical TTP transaction

An example of the steps of a secure transaction within the environment of the Public Key Infrastructure, is described in Figure 1. The most commonly adopted schema is the ‘on-line’ communication with the TTP rather than the ‘off-line’, which is not suitable for the support of on-line services, or the ‘in-line’, in which case the TTP interferes in every communication between the transacting parties. Furthermore, this schema adopts the TTP-to-TTP cross-certification, which proved to be the most reliable method in the projects

examined, rather than the user-TTP cross-certification. The latter, although it offers the shortest certification path, requires from the end-user to have the technical ability and the legal status to recognise all the possible standards and formats of the services offered by any TTP.

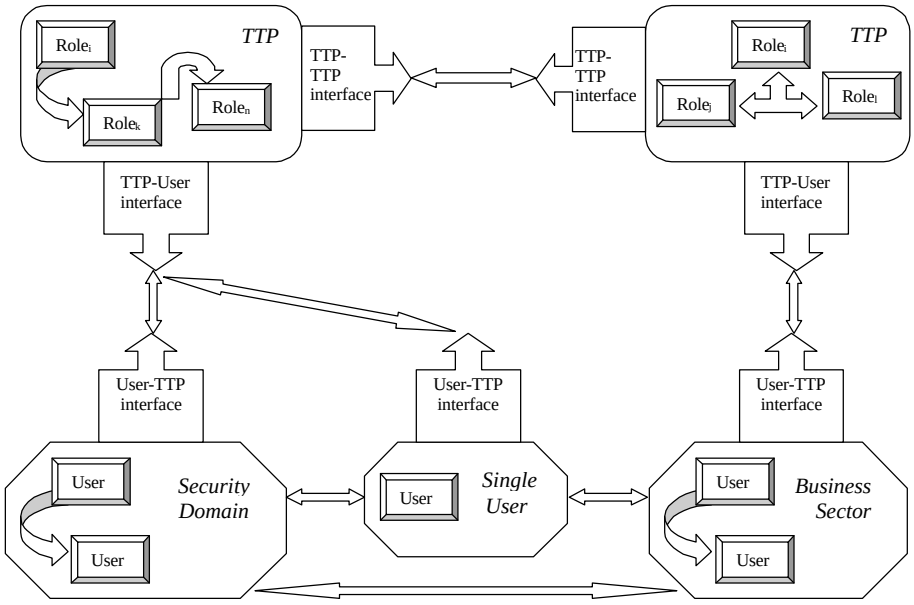

Figure 1. A typical TTP secure transaction

Step 1: Both users involved in the sample transaction are registered with the TTP of their domain (country or business sector etc.) and therefore a "Trusted Link" is established between each user and her/his TTP.

Step 2: The first user sends a message to the second user, which is digitally signed using her/his private signing key.

Step 3: The recipient requests information about the sender, from her/his home TTP.

Step 4: The TTP of the recipient re-routes the request for information to the TTP of the sender through a valid certification path, which may be direct or may include other higher-level TTPs. The request is signed with the private key of the recipient's TTP.

Step 5: The TTP of the sender responds to the request by returning the valid certificate of the sender or by stating that the certificate of the sender is not valid. In any case the response is digitally signed by the TTP with its private key.

Step 6: The TTP of the recipient validates the response and returns it to the requester signed in turn with its private key.

Step 7: The recipient validates the response using the public key of her/his TTP. She/he is finally able to check the validity of the received message by using the public key of the sender, which is included in the returned certificate, whose authenticity and integrity is guaranteed by her/his home TTP.

3. OVERVIEW OF RELEVANT INFOSEC AND ACTS PROJECTS

3.1 THIS: Trusted Health Information Systems

Information technology involved in the public health care sector is widely used for the management and communication of healthcare records and other sensitive information, requiring anonymity and protection against attacks.

The main objective of the project was to specify and define the health care sector requirements for the security services that must be offered and to propose a specific electronic signature solution associated to Trusted Third Party services.

3.2 Trusthealth-ETS

This project aimed to implement trustworthy information systems in health care to facilitate the secure exchange of information. It provided a set of specifications for security services and interfaces and a TTP service infrastructure operational in many countries and publicly available. The security services offered were based on the user requirements as described in project “THIS”.

Some of the issues that have been treated as important ones in Trusthealth-ETS are the operational electronic proof of authenticity throughout Europe and the assurance of an internationally unique, coherent and acceptable scheme. It introduced a Public Key Infrastructure specially designed for the health care sector, enabling the health professionals to communicate securely one with another and to have access to patients data. The implementation proposed was based on certificates specific for health care and on directory services.

3.3 TESTFIT

The field trial of TESTFIT was addressed to a specific user community, that of the public transport and international freight forwarders. However, the general objective of the project was to implement a solution using the TTP/ES approach to meet the security needs for a variety of users across Europe, to provide a standard for the inter-connection of TTPs and to promote the Electronic signature services to a wide user community.

The pilot implementation involved a trial with freight forwarders, transport operators and railway companies. It introduces the 'Security Message Headers' for the exchange of documents and includes several considerations on legal and regulatory aspects, quality aspects, as well as on the utilisation of the results of other relevant projects and of the internationally acceptable standards.

3.4 BOLERO

Bolero was specialised in the community of shipping and international transport. The main objective of the project was to implement a solution, by using the TTP/ES approach, to provide an electronic equivalent of negotiable documents used in international trading such as the 'Bills of Lading', 'Airway Bills' and other maritime official documents.

The project dealt with technical, legal and commercial aspects of a commercial transaction within the shipping industry. It is important to mention that prior to this study, there was no acceptable electronic equivalent of the negotiable documents, due to the legal difficulties faced, such as:

- the possession of a 'Bill of Lading' usually is equivalent to the ownership of the cargo,
- the document is 'negotiable' that means an entire cargo can change ownership by just consigning the Bill of Lading to another party or the same document may be officially presented in a court,
- banks are involved and money transactions are dependent on the presence of such a document, and
- the legal issues governing the use of Bills of Lading needed to be reviewed for the acceptance of the electronic form.

3.5 EBRIDGE

Provided Electronic Signatures (ES) and TTP enhancements to the EBR project, which in turn set up national company registries providing information to the public. The objectives of the project were:

- to demonstrate the feasibility of integration of ES technology to an already existent information retrieval infrastructure and the management of such a service,
- to evaluate the security offered by the field trial and indicate additions necessary for a secure operational service,
- to prepare and suggest the legal, regulatory and contractual framework within the field trial (and a future operational service) will operate, and
- to establish a Common Interest Group (CIG) that would both test the acceptability of the project principles and further spread the awareness of the results of the project.

3.6 EAGLE

The main objectives of this project were to study commercial, licensing and regulatory issues related to TTP services as well as the practicality and feasibility of a commercial TTP service. The EAGLE project studies in particular the potential services and features which could be offered by a pan-European network of TTPs and the potential technical mechanisms for key management for confidentiality services including the option of key recovery. Furthermore it examined the regulatory situation in the participating countries, surveying existing practices, current and future legislation, and reporting on any differences and conflicts

3.7 S2101

The prime objective of the S2101 project was to contribute to the strategic framework for the security of information systems, to the identification of user requirements and to the development of specifications and standardisation with respect to the security of information systems. The project was charged with producing a framework for the user requirements capture process, the guidelines for the management of TTPs and a functional model proving its validity.

3.8 ABS

The aim of ABS (Architecture for Brokerage Service) project was to design, implement and validate an open brokerage architecture for the provision of on-line information services, in the context of electronic commerce. The trials involved the participation of end-users, of a large number of National Hosts and of several Internet-based content providers.

Two main trials were organised. The purpose of the first trial was to validate basic functionalities like the combination of different sources to

generate a complex user request, the user interface, user request processing and request registration. The second trial involved services such as dynamic search execution, interfaces to supporting services and the federation of brokers. This test was addressed to user groups formed by the existing customer base of the content providers involved in the project.

3.9 GAIA

The GAIA (Generic Architecture for Information Availability) project developed a sector and supplier independent Generic Architecture for Information Availability, to support multilateral information trading. The GAIA architecture facilitates the location and delivery of information, products and digital services through a scaleable brokerage model broadly applicable to distributed information supply chains and networks. The project demonstrated applicability in three sectors: Music, Publishing and Technical Data.

3.10 OSM

The "Open Service Model for global information brokerage and distribution" project built an object oriented framework for globally distributed electronic commerce based on CORBA. The system includes an extensible set of object facilities and desktop components for building open electronic marketplaces. User and Service Centred Trials were undertaken in the area of news, media, content management and delivery.

4. TTP REQUIREMENTS

4.1 TTP user requirements

In this section we present — as a joint result of the user requirements capture processes of the examined projects — a unified and complete set of functional and non-functional end-user TTP service requirements.

Authentication: The accurate identification of the parties involved in various transactions or requesting documents storage and retrieval. This is implemented by using asymmetric cryptography (key pairs) for the electronic signing of a message and in many cases with the smart cards as a means of key storage.

Data Integrity: A message is not altered during its transmission through the electronic means, maliciously or accidentally. The integrity of sensitive

documents in all the examined sectors of health care, public transport and brokerage systems is seen as an important requirement. The solutions proposed are based again on electronic signatures and on hash-generating algorithms.

Confidentiality: Encryption of messages that must not be disclosed to any irrelevant party is mentioned as a major requirement in many projects; however only few implementations have taken place due to the legal complexities faced in most countries. The implementations are usually based on symmetric encryption keys and rarely on asymmetric key pairs. In the case of symmetric encryption, the key is incorporated in the digital signature of the sender.

Non-repudiation: A user cannot deny having sent or having received a particular message. Respectively we have the non-repudiation of origin and the non-repudiation of receipt, which are treated separately. Non-repudiation of origin is implemented using Electronic Signatures and in some cases by time-stamping. Non-repudiation of receipt is not implemented in any of the reviewed projects, although it is mentioned as a requirement. Only manual or automatic transmission of receipts is considered as a solution in some cases.

Availability: 24-hour 365-day service availability is also seen as a user requirement, since the service will be on-line, accessible through the network and applicable to different countries with different time-zones. Also the business sectors that a TTP service will apply such as Healthcare, transport and commerce are highly demanding as regards the availability of the information systems. Some projects have mentioned the necessity of a strong hardware background tolerant to break downs, with high availability.

Ease of use: System interfaces must be implemented in such a way that they would take into account the user friendliness, the applicability in many different business sectors and the linguistic and time diversity in Europe. The transparency of the certification procedures for the end user contributes also to the ease of use.

Mobility: Special provision is made in many cases for the mobile users. Roaming services are available, enabling the end-user to use the TTP services in the same way, regardless her/his location.

Anonymity: A user may require to retain her/his anonymity, although she/he is able to perform secure transactions. An entity may be registered with a TTP, but upon request, her/his personal details are not disclosed to anyone. This requirement is usually found in the health care sector systems.

Time-stamping: A reliable time-stamp, attached to the electronic documents exchanged between the users, is also seen as a requirement, in many circumstances. However, the time-stamping service, where offered, is seen as an auxiliary service or as an ‘add-on’, since it is not a pure security service, but it has indirect connection with other services, such as the non-repudiation service. Furthermore the implementation of time-stamping

services carries a high level of complexity, since they require reliable and expensive hardware time synchronisation procedures.

Uniqueness: The uniqueness of a commercial document (such as a negotiable Bill of Lading) in electronic form is also seen as a requirement, especially by the projects dealing with the public transport sector. It is required that the original document can be always identified, as well as the current holder of the document.

Interoperability: Secure message exchanging cannot be restricted within one domain. It is required that secure messages can be sent across domains, between users who are registered with different TTPs.

Protection from abuse: Abuse of the TTP infrastructure should be difficult and where possible detectable. Physical and electronic Access control lists must be implemented.

Legal and Notary: The requirement of the users to have sufficient legal protection and rules conformity with the official electronic documents, exactly like exchanging paper documents, is in-depth considered in many projects. An interesting proposal introduces the idea that the members of a TTP are forming an association and they must abide by its rules in order for the electronic documents they exchange to become acceptable in a jurisdiction. Another legal requirement is that the TTP should implement policies and mechanisms for dispute resolution.

Accreditation: The auditing procedures for a TTP are considered as essential for the unobstructed operation and for the trustworthiness of the system. A generally accepted organisation in a pan-European scale should act as a certification authority for the TTP and create the necessary accredits.

Compatibility and Portability: It is necessary for the system to be designed in such a way that it would be compatible with the most widely used technologies and able to easily adopt any newer variation of the established technologies.

Security policy: The TTP is requested to present to its users a well-defined security policy, that will accommodate both national constraints and regulations as well as the security objectives related to the business sector it is addressed to.

Modularity: The infrastructure required for the TTP services should be scaleable in an economic way and manageable in large scale implementations. Furthermore, the services offered must be implemented in the system in a modular way, enabling the addition or subtraction of service modules.

Key management: Either the end-user or the state itself, will request from the TTP various services related to the signing and confidentiality keys (if they are different). These include key generation, key distribution — usually with out-of-band mechanisms, key recovery (when a key is lost, or by court decision, or when an organisation demands access to files encrypted by its

employees) key backup, key escrow (surrendering keys to a third party upon law enforcement), and automatic key update upon expiration or compromise.

Directory services: It is a necessary part of the TTP systems, for distributing the public keys and the certificates of the registered users and for making them publicly available. The availability of public keys and Certificate Revocation Lists (CRLs) is an essential for the certification/validation process. Directory services should be implemented under the widely deployed standards such as X.500, LDAP, DNS.

Personal data protection: The TTP must abide by the rules already in force in several European countries regarding the protection of the sensitive personal data, wherever such data could be found massively stored.

Out-of-band communication: Out-of-band communication mechanisms such as the delivery of smart cards or conventional mail are necessary at the early stages of user registration before 'Trust' is established between the TTP and the user.

On-Line services: Finally, the end-users will require the provision of some on-line services such as registration, billing, and the availability of a help-desk.

4.2 TTP legal requirements

All the examined projects are concerned about various organisational, legal and regulatory issues that will assist the TTP to establish Trust within the domain they deal with. It is a common idea that the regulations that govern a TTP are affected by legislation specific to each country and by the rules and practices followed within a business sector or domain. The common market implies the free mobility of professionals, goods, and consumers from different sectors such as health care, transport, and on-line services. As the law concerning this mobility itself and the electronic means for their secure and lawful transactions varies considerably along European countries the projects were required to provide harmonised solutions.

The main objectives of the examined projects were three:

- the compliance with national and international law,
- the 'binding' of the users of a TTP by certain rules and agreements that will enable the presentation of their transactions in a jurisdiction, as official documents, and
- the interoperability between different European countries and different business sectors, that will enable their users to perform lawful and official transactions.

In particular, the legal issues addressed and taken into account for the usage of TTP services are:

- the regulations about *the protection of private information* as recommended by various countries and by the European Union,
- the *secrecy of professional data,* which is found in European legislation in many variations,
- the provision of *evidence of authenticity* for the content and the originator of the electronic documents, which may be officially used in the state or in the court,
- the various state regulations about the usage of *cryptographic products* and specifically the export and the personal use,
- the concept of '*Ownership'* in medical data and in shipping documents, such as the 'Bills of Lading', and
- the creation of official *Associations of users*, who will abide by their rules and who are clearly stating full trust to the TTP. The association aims to create a legally binding electronic signature, which is capable of full and unconditional acceptance by a judge.

The conclusion derived from the legal requirements studied in the INFOSEC projects is the need for a dispute resolving mechanism. Often in the commercial world the contents of contracts and agreements are worthless pieces of paper until a dispute arises; at that point a TTP must provide adequate solutions. The majority of the projects accept as a solution the formation of bilateral commercial agreements between the service providers and the users, as well as between different service providers, for interoperability purposes.

5. CONCLUSIONS

All the aforementioned projects may be mapped onto an abstract reference model as described in the 'Keystone' project. The various activities performed within a TTP for the provision of its services can be clustered in *roles*. These roles can be defined as integrated actions performing specific well defined tasks in order to provide, probably in interaction with other entities and roles, trust services in open distributed systems. The roles are of little use if used separately. They represent the individual actions, which comprise trusted services. Examples of individual roles are the 'Key management', the 'Customer oriented services', the 'Trust enhancement and management role', the 'time-stamping services' and the 'Certification role'.

The organisational entities involved in transactions, i.e. the 'actors', are the users and the TTPs. Trust services are offered by the TTPs to the users at the TTP-User interface. Roles perform specific well-defined individual tasks, and several roles co-operate in order to provide security services to meet specific user requirements and therefore implement trust service. TTPs in

different domains must be able to interact and co-operate with other TTPs in order to meet their user needs. The interaction between TTPs is performed at the TTP-TTP interfaces, usually called 'gateways'.

The specification of a common reference model for the Public Key Infrastructure in Europe is an absolute necessity, in order to merge the results of various projects concerned with TTP services in different sectors. Specifically, the user requirements for the TTPs are extracted and highlighted, as stated in the INFOSEC projects *THIS*, *TrustHealth-ETS*, *TESTFIT*, *BOLERO*, *Ebridge*, *EAGLE and S2101*, and in the ACTS projects *ABS*, *GAIA, and OSM*.

The user security requirements specified in the aforementioned projects proved to be similar, though the level of details and importance of particular requirements vary between different projects. Most of the projects specified the following minimal set of security services and requirements: authentication of users, integrity of messages, privacy and confidentiality of messages, non-repudiation of message origin and destination, availability of services, and ease of use. Additionally, the issues that have been recognised as important ones in some of these projects are anonymity of participants, time-stamping, uniqueness of documents, interoperability between different elements, protection from abuse of any participant by another, and legal issues.

The merged results gained in this context will provide the guidance and expertise required to provide a useful input to the TTP service development process, which is the link between the user needs and the functionality of the PKI.

REFERENCES

[ABS, 1996] ABS Broker Business Model, ABS Deliverable D2.3, 1996.

[ACTS, 1997] Advanced Communications Technologies & Services, Project summaries, 1997.

[BOLERO, 1995] BOLERO INFOSEC project final deliverable, 1995.

[Castell, 1993] Castell S., Code of Practice and Management Guidelines for Trusted Third Party Services, INFOSEC Project Report S2101/02, CEC/DG XIII/B6, 1993.

[EAGLE, 1997] INFOSEC EAGLE Deliverable #2, Assessment criteria for TTP services, October 1997.

[Ebridge, 1995] INFOSEC Ebridge Final Report, ES & TTP enhancements to EBR, 1995.

[GAIA, 1996] Generic & domain requirements statement, GAIA Deliverable 0301, 1996.

[GAIA, 1997] Design of the GAIA integrated security system, GAIA Deliverable 0801, 1997.

[IFIP, 1997] IFIP joint TC6/TC11 working conference on Communications and Multimedia Security, Volume 3, edited by Sokratis Katsikas, 1997

[KEYSTONE, 1998] KEYSTONE European Cross Domain Public-key Infrastructure Architecture project deliverables, 1998.

[Muller, 1993] Muller P., Functional Model of Trusted Third Party Services, INFOSEC Project Report S2101/03, CEC/DG XIII/B6, 1993.
[MULTIMEDIATOR, 1997] ACTS MULTIMEDIATOR deliverable D12, 1997.
[OPARATE, 1998] OPerational and ARchitectural Aspects of TTPs for Europe, INFOSEC-ETS project deliverables, 1998.
[OSM, 1997] OSM Broker, Banker, Dealmaker (Consolidated Analysis), OSM deliverable 6, 1997.
[TESTFIT, 1995] TESTFIT - TTP & Electronic Signature Trial for Inter-modal Transport, Final Report, INFOSEC Project Report S2303, CEC/DGXIII/B6, September1995.
[THIS, 1995] Trusted Information Systems THIS project, final deliverable V2.0, Requirements on Electronic Signature Services and TTP services, Swedish Institute for Health Services Development, Sweden, 1995.
[TrustHealth-ETS, 1996] Healthcare Telematics/TrustHealth-ETS project, Functional Specification of TTP Services, Swedish Institute for Health Services Development, Sweden, August 1996.