

Support for Legal Framework and Anonymity in the KEYSTONE Public Key Infrastructure Architecture

Ahmed Patel¹, Pavel Gladychiev¹, Sokratis Katsikas², Stefanos Gritzalis², and Dimitris Lekkas²

¹Department of Computer Science, University College Dublin, Belfield, Dublin 4, Ireland, email {apatel,pavel}@net-cs.ucd.ie : ²Department of Mathematics, University of the Aegean, Samos, Greece, email {ska,sgritz,dlek}@aegean.gr

Key words: Pan-European Public Key Infrastructure, Anonymity, Legal Framework, Digital Signatures, Directory Service, Public Key Certificates

Abstract: The paper describes the results of the KEYSTONE project developed a unifying reference model (framework) for integrating existing Public Key Infrastructure systems across Europe in a Pan-European Public Key Infrastructure. The major result of the project, the KEYSTONE architecture, is reviewed in this paper, and its elements supporting legal framework and anonymity of users are examined.

1. INTRODUCTION

The development of an open information society is impossible without protecting privacy and assets of individuals. Public Key Infrastructure (PKI) consisting of independent Trusted Third Party (TTP) institutions or organisations is an important security element of an information society. PKI provides services such as public key certification, and time-stamping of digital documents to facilitate security, protection and safety.

A lot of work has been done over the past several years towards development and standardisation of specific PKI services. As a result, a number of pilot systems were deployed world-wide and their use is increasing. At the present time, there is a great demand in Europe to integrate exiting PKI services and systems in a consistent and easy-to-use

Pan-European PKI. One of the main aims of the KEYSTONE project was to propose a logical architecture for Pan-European PKI that would allow such integration. The PKI architecture developed within the KEYSTONE project addresses many aspects of the PKI. It proposes generalised models and technological solutions addressing access to PKI services, internal functioning of a TTP, and the overall functioning of a Pan-European PKI. The discussion of the KEYSTONE architecture and its features supporting legal framework and anonymity of users is the central topic of this paper.

The discussion is divided into three sections. The next section outlines the key elements of the KEYSTONE architecture. After that, Section 3 examines key features of the KEYSTONE architecture supporting legal framework and anonymity of users. Finally, the fourth section concludes the paper.

2. KEYSTONE ARCHITECTURE

KEYSTONE architecture is a generalisation of earlier PKI architectures envisaged by a number of European projects including among others BOLERO [1], TESTFIT [10], and Ebridge [2] projects.

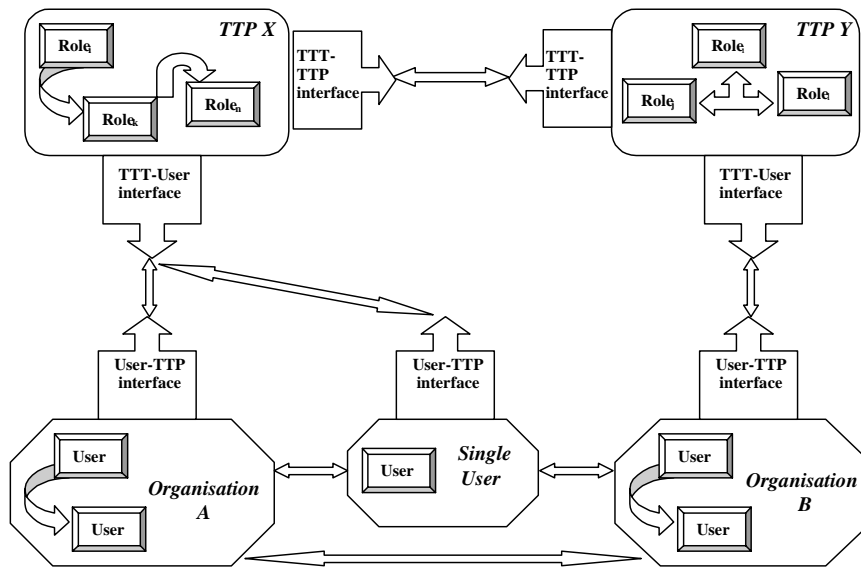


Figure 1. KEYSTONE Reference Model

The high-level structure of the Pan-European PKI is captured in the KEYSTONE Reference Model [6] depicted in Figure 1, which is flexible to cater for all kinds of users, suppliers of ordinary services, PKI services and inter- and intra- interworking operations.

Two types of organisational entities are identified: *Trusted Third Parties* and *PKI users*. Each TTP serves needs of one or more administrative domains. A TTP offers PKI services to its users at the TTP-User interface. When users of different TTPs need to interact, TTPs serving these users cooperate. The interaction between TTPs is performed through the TTP-TTP interface.

2.1 PKI services

As a part of the KEYSTONE architecture development, user requirements for Pan-European PKI services were captured [11,8]. The typical comprehensive list of PKI services required for a Pan-European PKI by its potential users are:

1. *Registration*. In order for a user to join the PKI environments s/he must register with a certifying TTP belonging to the PKI. The primary goal of this service is to establish the reliable unique binding between a user and her/his public key.
2. *Digital signatures*. In order to satisfy the message authentication, message integrity and non-repudiation of origin user requirements, the PKI should offer digital signature services.
3. *Encryption*. Encryption is a basic service providing the cryptographic functions for protection of message confidentiality in a computer network.
4. *Time-stamping*. Time stamping is described as the process of attaching data and time to a document in order to prove that it existed at a particular moment of time.
5. *Non-repudiation*. Non-repudiation involves the generation, accumulation, retrieval, and interpretation of evidence that a particular party processed a particular data item. The evidence must be capable of convincing an independent third party, potentially at a much later time, as to the validity of a claim.
6. *Key management*. This service deals primarily with the handling of cryptographic keys in a proper, efficient, scalable and secure way. It includes key pair generation, key archiving, key backup, key pair renewal, and some other functions.

7. *Certificate management.* A digital certificate is an electronic token ensuring the binding between an entity and its public key. The functions of this service cover generation, distribution, storage, retrieval, and revocation of digital certificates.
8. *Information repository.* This service maintains the collection of data critical for the operation of the TTP system. It states the general means and fashion for storing, archiving and maintaining several types of data ranging from organisation's legal requirements, to system recovery needs.
9. *Directory services.* In order to interact, a member of PKI must have access to the useful information about other PKI members. This is achieved by the use of Directory services.
10. *Camouflaging communications.* A camouflaging communication not only provides data confidentiality, but also hides the very fact of communication. This is achieved by adding dummy messages into the data stream enabling TTPs and users to hide real data transfers, both in terms of their occurrence and frequency. This service is provided by a group of co-operating TTPs forming a camouflaging network.
11. *Authorisation.* The PKI should enable requesting entities with the right to delegate access rights at will to other PKI entities. This means that a PKI user who possesses a resource may grant the right to another PKI user to access this resource. TTPs should ensure the granting of rights, including the ability to access specific information or resources.
12. *Audit.* In order to ensure that certain operational, procedural, legal, qualitative and several other requirements are complied with so that trust is enhanced, auditing service is required.
13. *Quality assurance and trust enhancement services.* It is expected that the potential users of PKI services, would require products and services of a given quality to be delivered or be available by a given time and to be of a price which reflects value for money. In order to achieve this level of quality, quality assurance of PKI services is required.
14. *Customer oriented services.* This group of PKI services includes services, which directly involve users or need some contact, or some kind of dealing or bargaining with the end user. Those are the services like legal aspects and payment negotiations between a user and a TTP.
15. *TTP to TTP interoperability.* In the Pan-European Public Key Infrastructure it is unlikely that all users will be connected to a unique TTP. Interoperability services are concerned with the issues necessary for establishing a network of TTPs possibly operating by different companies with different policies and different domain specialisation.

However, it is important to note that only a few of the above listed services will be required by a particular application at any one time. For example, non-repudiation service will be essential for electronic document processing, but it will not be used by simple privacy enhanced e-mail applications. The task of defining all the essential PKI services for end-user applications is beyond the scope of this paper.

2.2 TTP roles

The KEYSTONE architecture also identifies the specific tasks called TTP roles that must be performed within the TTP to provide PKI services. The KEYSTONE architecture identifies eight such roles:

1. *The time-stamping role (TS)*. Time-stamping role is responsible for fulfilling the PKI community requirement for valid transactions and unique documents sets. Time-stamping role can be seen as a transaction notary, which commits the fact of existence and correctness of a document and a transaction respectively, by producing, storing and verifying time-stamped documents. It is highly possible that the role should be performed by an independent and trustful entity providing indisputable time-stamps.
2. *Management and trust enhancement role (MT)*. Management and Trust enhancement role could be simply considered as the administrative department of a trust-based organisational system. The basic duties of this role include establishment of a TTP organisational structure; establishment, operation and management of quality assurance and audit plans; establishment and enforcement of organisation's policies, etc.
3. *Legal issues management role (LI)*. Legal issues management role is responsible for study of the existing legal context of the PKI operation, contribution to the emerging legal frameworks and monitoring of the PKI operation, in order to handle legal issues or possible problems in either PKI-User or TTP-TTP relations.
4. *Key management role (KM)*. This TTP role is related to the key management functions supported by the TTP. The key management role has a number of duties such as key generation, key certification, key distribution, key revocation, key escrow/recovery, key translation, key storage and backup.
5. *Customer support role (CS)*. This TTP role is involved in the provision of services, which are addressed directly to the end-users who need any kind of contact, support (technical, informational, financial etc.) or some kind of dealing or bargaining. Examples of the duties of this role are client

charging and billing, dispute handling and resolution, and 24-hrs Help desk and Hot-line.

6. *Accounts management role (AM)*. Like every organisation or company, the TTP is obliged to have a role involved in the internal accounting, according to certain rules applied e.g. by governments and local tax authorities. Its duties are to insure that imposed accounting controls are strictly followed, to propose a proper way of asset management, to ensure that only valid transactions are processed and recorded in the accounting records, etc.
7. *Registration role (R)*. This role is responsible for actions performed when a new entity subscribes for TTP services. The activities involved with the every day operation of this role include evaluation of registration forms and supporting documents, authentication and identification of candidate entities, user anonymity assurance, notification of candidate entities about evaluation results, etc.
8. *Certification role (C)*. This role forms the heart of each TTP. The ultimate goal of this role is to effectively manage the certificates generated and revoked by the TTP. Its duties involve certificate generation, certificate storage and retrieval, maintenance of certificate revocation list, storage and retrieval of certificate revocation list.

The relationship between the PKI services and the TTP roles is given in Table 1, below.

Table 1. Relationship between PKI services and TTP roles

PKI service	TTP role	TS	MT	LI	KM	CS	AM	R	C
Registration				+				+	
Digital signatures		+		+	+				+
Encryption			+	+	+				+
Time-stamping		+		+					
Non-repudiation		+		+					
Key management			+	+	+				+
Certificate management				+					+
Information repository			+	+					+
Directory services			+	+	+				+
Camouflaging communications			+	+	+				
Authorisation			+	+				+	
Audit			+	+					
Q.A. & Trust Enhancement			+	+					
Customer oriented services				+		+	+	+	
TTP to TTP interoperability				+	+			+	+

A '+' sign in the table indicates that a TTP role is involved in the provision of a specific PKI service.

The TTP roles do not separate human and technical aspects of the TTP, thus, delivering a comprehensive high level picture of the TTP functioning. The separation of human and technical concerns is addressed in more technical components of the KEYSTONE architecture.

2.3 Other components of the KEYSTONE architecture

The KEYSTONE Reference Model, PKI services, and TTP roles form a high-level description of the KEYSTONE architecture. Other parts of the KEYSTONE architecture describe specific components of the architecture in more detail. Much of this is beyond the scope of this paper. However, for the sake of completeness, these include:

1. *TTP Functional Architecture*: describes internal functioning of the technical component of a TTP at the level of functional units interacting across clearly defined interfaces [5]. Functional units are basic blocks of the TTP Functional Architecture. They provide services to one another by means of abstract primitives, operations that they carry out for one another. Each functional unit exports a number of abstract primitives to the others, and imports some abstract primitives from the others. For example, the Cryptographic Services functional unit exports abstract primitives for encryption, decryption, and digital signature generation and verification. The Electronic Payment Mechanisms functional unit uses (imports) these abstract primitives to implement abstract primitives for electronic payment.
2. *Technology Profile*: analyses available PKI technologies and recommends the most suitable candidates for use within the Pan-European PKI. The KEYSTONE technology profile is described in [7].
3. *Interoperability Solutions*: include a number of protocols and data formats [9] proposed by the KEYSTONE project to facilitate interoperability within the Pan-European PKI. These solutions bridge the gaps between existing and new PKI standards. They also provide an evolutionary migration path with a high degree of PKI service availability.

These components are essential to determine engineering aspects of the PKI services.

3. LEGAL RELATIONSHIPS AND ANONYMITY

The non-technical, but very important aspect of PKI and TTPs is the legal framework, which determines rights and responsibilities of TTPs and PKI users and defines ways for civilised conflict resolution within the Pan-European PKI.

The support for legal framework and anonymity of users is present throughout the KEYSTONE architecture. Key features serving this purpose are:

1. the use of digital signatures in the KEYSTONE generalised service protocol,
2. standardised format for information about legal conditions of all PKI services,
3. anonymous public key certificates.

3.1 Digital signatures in the protocol for generalised PKI service

Although the protocols for PKI services are widely studied and standardised, they are somewhat limited in the sense that they do not cover all aspects of interaction between a TTP and its client. For example, the ITU-T X.509 [3] recommendation defines the authentication scheme and the digital certificate format, but does not define actual protocols for reporting a private key compromise, or for billing a TTP customer.

In order to achieve consistency and fill gaps in existing protocols, the KEYSTONE architecture has defined the following generalised scheme of service provision. It can be seen as a ‘metaprotocol’ that uses existing protocols to perform specific tasks. The functioning of the protocol is divided into six stages:

1. *Initialisation.* The service provision begins with a PKI user submitting a Service Request message to a TTP. The purpose of the service request is similar to a paper based order form. It facilitates service provision and carries information typically present in usual order forms:
 - Service description
 - Service delivery method description
 - Payment method description
 - Invoice and receipt delivery method description
 - Date and time
 - Requester’s identification and digital signature

- Additional information (e.g. public key certificates)
- 2. *Request verification.* After receiving a service request, the TTP analyses it. The requester's identity is authenticated, and his right to request a particular type of service is verified. If there is any problem, the TTP replies to the service requester with a digitally signed Error Message stating the problem. The service provision is terminated. If there is no problem with the service request and if no payment is required, steps 3 to 5 are skipped and the TTP proceeds to the service provision phase, otherwise the protocol proceeds to the step 3.
- 3. *Invoice.* If the requested service is not free of charge, the TTP sends to the service requester an Invoice message specifying service details and the price involved.
- 4. *Confirmation.* After receiving an invoice the service requester should either confirm or reject the offer by sending a Confirmation message. If no decision is made after a certain period of time, the TTP assumes a negative answer, and the service provision is terminated.
- 5. *Payment.* After confirmation is received, the TTP and the service requester perform the payment procedure, which can be done either on-line or off-line (e.g. from the user's account with the TTP). After completion of the payment procedure, the TTP sends a Receipt message to the customer, which indicates the accepted amount of money, and confirms the responsibility of the TTP to perform the service.
- 6. *Service provision.* After the payment is complete (if required), the TTP performs the requested service, and delivers it to the service requester via the specified delivery method.

Digital signature of a TTP or a PKI user is a mandatory element in all messages exchanged in the protocol. The messages can be considered legally binding in countries where digital signatures and digital documents are accepted as a substitute for paper based documents. Where it is not legally binding, it can be used as evidence to prove transaction commitment.

3.2 Information about legal conditions of PKI services

The KEYSTONE architecture is decentralised. It does not define a strict set of policies or PKI services that must be implemented by a TTP in order to join the Pan-European PKI. Instead of this, the KEYSTONE architecture provides a way for PKI users to get precise information about technical parameters and legal conditions of PKI services offered by a specific TTP.

This is achieved by placing a record into the X.500 directory [4] about each TTP participating in the Pan-European PKI. The KEYSTONE

architecture defines a standardised format for such a record. It contains the following information about a TTP:

1. A list of supported PKI services and their parameters.
2. A list of supported methods for accessing PKI services (e.g. WWW, e-mail, postal mail, etc.) and parameter of those methods.
3. A list of supported payment methods (e.g. by credit card, by cheque, etc.) and their parameters.
4. A list of supported methods for PKI service delivery (e.g. on-line, by postal mail, by e-mail, etc.) and their parameters.

Most importantly, every description of a supported PKI service includes a mandatory field explaining the legal conditions under which the service is provided. This field can either be a verbal description or it can refer to some official document such as a standard or legal regulation.

3.3 Support for anonymous transactions

The user requirements study carried out by the KEYSTONE project [11] demonstrates that anonymity is important in a number of electronic services. It is especially important in electronic commerce and citizen-to-government transactions, where anonymity gives an individual a degree of protection against persecutions. KEYSTONE architecture addresses the anonymity requirement by providing anonymous public key certificates.

In the KEYSTONE architecture a user may ask the TTP to put an alias in the public key certificate instead of his/her real name. The use of an alias 'anonymises' electronic services that authenticate users by their public key certificates.

This approach provides low degree of anonymity, because the link between the true identity of the person and his/her alias is known to the TTP, and hence can be obtained from the TTP either legally or illegally. This approach can, however, be advantageous, because it allows the law enforcement to easily find the true identity of the person if necessary [13,14].

4. CONCLUSIONS

The foregoing has described the logical architecture for the Pan-European Public Key Infrastructure developed by the KEYSTONE project. The KEYSTONE architecture provides a unifying framework for integration of existing PKI systems across Europe in a Pan-European PKI and creates a

solid base for the development of the Pan-European PKI in the future. Among other technical solutions, the KEYSTONE architecture includes a number of features supporting legal framework and anonymity of users. The paper has described three of them: the use of digital signatures in the KEYSTONE generalised service protocol, standardised format for information about legal conditions of PKI services, and anonymous public key certificates.

The results of the KEYSTONE project have been partially submitted to the European Standardisation Committee (CEN) subcommittee 251 and to the Internet Engineering Task Force (IETF) as a draft proposal for a new PKI framework standard. At the present time, the authors are preparing a follow-up project that would develop technological solutions proposed in the KEYSTONE architecture. This would be a pilot prototype to validate the key concepts of the KEYSTONE architecture and verify its technical solutions.

ACKNOWLEDGEMENTS

We wish to thank the European Union for funding the KEYSTONE project.

REFERENCES

1. BOLERO. Final Report', BOLERO Consortium, 1995, <ftp://ftp.cordis.lu/pub/infosec/docs/s2302.zip>
2. 'ES & TTP enhancements to EBR', Ebridge project final report, Ebridge Consortium, 1995, <ftp://ftp.cordis.lu/pub/infosec/docs/s2301.zip>
3. 'Information technology – Open systems Interconnection – The Directory: Authentication framework', ITU-T X.509 Recommendation, International Telecommunication Union, 1997
4. 'Information technology – Open systems Interconnection – The Directory: Overview of concepts, models and services', ITU-T X.500 Recommendation, International Telecommunication Union, 1997
5. 'Keystone Functional Architecture' Deliverable 5.1, KEYSTONE Consortium, 1998
6. 'Keystone Reference Model' Deliverable 4.1, KEYSTONE Consortium, 1998
7. 'Keystone Technology Profile' Deliverable 7.1, KEYSTONE Consortium, 1998
8. 'Service Scenarios Definition' Deliverable 2.1, KEYSTONE Consortium, 1998
9. 'Standards Submission' Deliverable 8.2, KEYSTONE Consortium, 1998
10. 'TESTFIT - TTP & Electronic Signature Trial for Inter-modal Transport', Final Report, TESTFIT Consortium, 1995, <ftp://ftp.cordis.lu/pub/infosec/docs/s2303.zip>
11. 'User Requirements Report' Deliverable 1.1, KEYSTONE Consortium, 1998

13. Muftic, S., *et al* 'Security Architecture for Open Distributed Systems' John Wiley and Sons, Chichester, 1993, pp. 281, ISBN 0 471 93472 0
14. Muftic S., *et al* 'Security Mechanisms for Computer Networks' Ellis Horwood Limited, Chichester, 1989, ISBN 0 7458 0613 9