BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

ORGANISATIONAL FRAMEWORK IMPLEMENTATION

VERSION 1.0

ECB-Restricted
24-Jan-2012

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

Project name:	ESCB-PKI
Author:	ESCB-PKI Project Team
File name:	ESCB-PKI - Organizational Framework implementation V.1.0.docx
Version:	1.0
Date of issue:	24.01.2012
Status:	Draft
Approved by:	
Distribution:	

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	Status	Date of issue	Revisions
0.1	Draft	20.10.2011	Initial version.
0.2	Draft	14.11.2011	BdE Revision
0.4	Draft	28.11.2011	BdE Revision
0.5	Draft	22.12.2011	BdE Revision
1.0	Draft	24.01.2012	Version for SRM-WG revision

GLOSSARY AND ACRONYMS

Acronym	Definition
AA	Access Administrator.
BdE	Banco de España (Bank of Spain).
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
Customer	Customer is defined as the entity (Level 1 – Eurosystem) that has a business relationship with the service providing organisation, receives, uses and is directly affected by the services of the service providing organisation.
Directory	Data repository that is accessed though the LDAP protocol.
Electronic Certificate	Document signed electronically by a Certification Service Provider, which links signature verification data (public key) to a signatory and confirms their identity. This is the definition contained in Law 59/2003, which this document extends to cases in which the signature verification data is linked to a computer component.
ESCB	European System of Central Banks.
HSM	Hardware Security Module: cryptographic security module used to store keys and carry out secure cryptographic operations.
IAM	Identity and Access Management. In the context of this document, IAM is referred to IAM ESCB project.
Identification	The process of establishing the identity of an applicant or subscriber of an ESCB-PKI certificate.
ITC	Information Technology Committee.
KRO	Key Recovery Officer.
LDAP	Lightweight Directory Access Protocol.
LSO	Local System Owner.
PAA	Policies Approval Authority.
PIN	Personal Identification Number: password that protects access to a cryptographic card.
PKI	Public Key Infrastructure.
Public Key and Private Key	The asymmetric cryptography on which the PKI is based employs a key pair in which what is enciphered with one of these keys can only be deciphered by the other, and vice versa. One of these keys is "public" and includes the electronic certificate, whilst the other is "private" and is only known by the certificate subscriber and, when appropriate, by the Keys Archive.
Public Key Infrastructure	Set of individuals, policies, procedures, and computer systems necessary to provide authentication, encipherment, integrity and non-repudiation services, by way of public and private key cryptography and electronic certificates.
PUK	PIN UnlocK Code: password used to unlock a cryptographic card that has been locked after repeatedly and consecutively entering the wrong PIN.
RA	Registration Authority.
Relying Parties	Individuals or entities other than subscribers that decide to accept and rely on a certificate issued by ESCB-PKI.
RO	Registration officer.
RO4EO	Registration officer for external organisations.
RO4TC	Registration officer for technical components.
SO	System Owner.
Subscribers	Individuals or computer components for which an electronic certificate is issued and accepted by said individuals or, in the case of component certificates, by the component manager.

TCS	Technical certificate subscriber.
Third party	Also called Third party service provider, i.e. a company recognized as being independent of the parties involved (Service providing organisation and Customer) that provides services generally covered by a Service Level Agreement.
User	A user is an individual that can log into the service with a login name and requests or uses the services provided.

1. INTRODUCTION

A Public Key Infrastructure (PKI) is a technology, together with the relevant operational, registration, revocation and other certificate management procedures. It is used to assure the security and protection of electronic communications and of data stored electronically, by means of the use of pairs of public and private keys.

The ESCB Public Key Infrastructure (ESCB-PKI) will provide the certificates necessary to comply with the IAM Security Policy requirements and to offer other advanced security features such as encryption and digital signature. The types of certificate subscribers to be considered in the project are:

- ESCB users;
- non-ESCB users;
- ESCB/CB applications and technical components.

On the other hand, the services provided by the ESCB-PKI are:

- Certificate Management Service;
- Registration Service;
- Revocation Management Service;
- Key Recovery Service;
- Cryptographic Token Management Service.

The purpose of this document is to present an overview of the organisational framework for the ESCB-PKI solution, describing the participants and their responsibilities.

Further details of the framework are fully described in the ESCB-PKI Certification Practice Statement (CPS) and in the Certificate Policies (CP) associated to each certificate type issued by the ESCB-PKI. These documents are available in the ESCB-PKI Website.

2. ASSUMPTIONS AND DEPENDENCIES

Before dealing with the actual organisational framework this section will discuss about those policies and regulations upon which ESCB-PKI relies and by which the framework shall abide.

2.1. ESCB INTERNAL POLICIES

The ESCB-PKI, like any other ESCB project, must comply with all ESCB applicable policies; among others, the following policies are considered:

- ESCB Information Systems Security Policy;
- ESCB Network Security Policy;
- ESCB Identity and Access Management Policy;
- ESCB Vulnerability and Patch Management Policy;
- ESCB Logging and Monitoring Policy;
- ESCB Certificate Acceptance Framework;
- ESCB ITSM Policies.

2.2. PKI STANDARDS

European standards related to PKI are also to be taken into consideration, among those the most significant are:

- IETF RFC 5280 (Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List Profile);
- IETF RFC 3647 (Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework);
- IETF RFC 2560 (X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol);
- ETSI EG 200 351 v4.1.1 (ETSI object identifier tree; rules and registration procedures);
- ETSI TS 102 176-1 v2.0.0 (Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms);
- IETF RFC 3739 (Internet X.509 Public Key Infrastructure: Qualified Certificates Profile);
- ETSI TS 101 862 v1.3.3 (Qualified certificate profile);
- ETSI TS 102 280 v1.1.1 (X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons);
- ETSI TS 101 456 v1.4.3 (Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates);
- ETSI TS 101 042 v2.1.2 (Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates);
- IETF RFC 4055 (Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile);
- CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures);
- CWA 14172 (EESSI Conformity Assessment Guidance);
- FIPS 140-2 (Security Requirements for Cryptographic Modules) Level 3;
- ISO/IEC 15408-3 (Common Criteria EAL4+).

2.3. EUROPEAN REGULATIONS

Legal and regulatory issues are of utmost importance in the implementation of a PKI. The most relevant are:

- European Parliament and Council Directive 1995/46/EC of 24 October 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- European Parliament and Council Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures.

2.3.1. DATA PROTECTION

The Data Protection Directive (1995/46/EC, 24 October 1995) was drawn up to address the need for pan-European flow of information and the need to have a minimum level of data protection when such information flows across borders. The Directive comprises a set of principles/requirements which make data processing lawful. Data minimisation has to be observed (art. 6), data processing needs to be adequate, relevant, and not excessive in relation to its purposes and data should be accurate and up to date.

The Directive provides a set of legal requirements for personal data to be processed throughout private and public services in Europe and has been transposed into national regulation by all Member States.

Even though there are differences in the transposition of the Directive in the different Member States, the principles laid down in the Directive are respected by all Member States. Therefore, the project specifications will be made based on this EU directive.

2.3.1. ELECTRONIC SIGNATURE

According to the Electronic Signature Directive (1999/93/EC, 13 December 1999) an ‘electronic signature’ means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. Therefore it is a technique by which it is possible to secure information in such a way that the originator of the information, as well as the integrity of the information, can be verified.

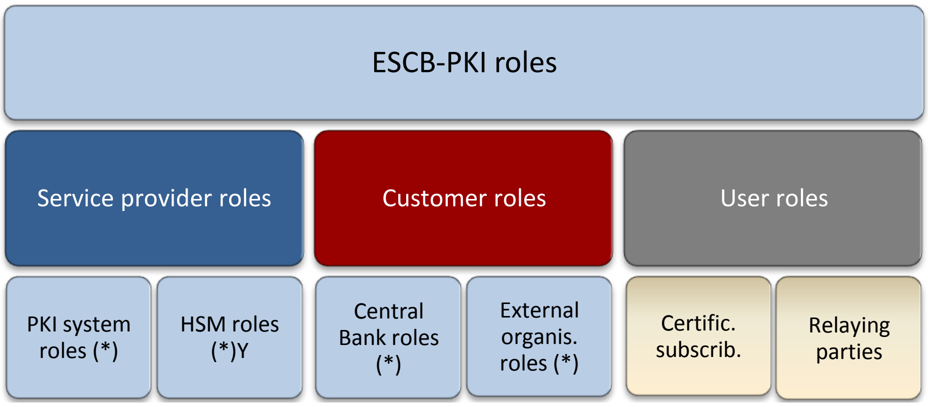
The term ‘advanced electronic signature’ means an electronic signature which meets the following requirements:(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

An electronic signature is to be treated legally equal to a hand-written signature when it concerns an: (a) advanced electronic signature based on (b) a qualified certificate and (c) created by a secure-signature-creation device.

3. ESCB-PKI ROLES

This chapter describes the roles that are required to implement the ESCB Public Key Infrastructure:

- Service provider roles;
- Customer roles;
- User roles.



(*) These are role classifications. For the sake of readability, roles that belong to them are described later.

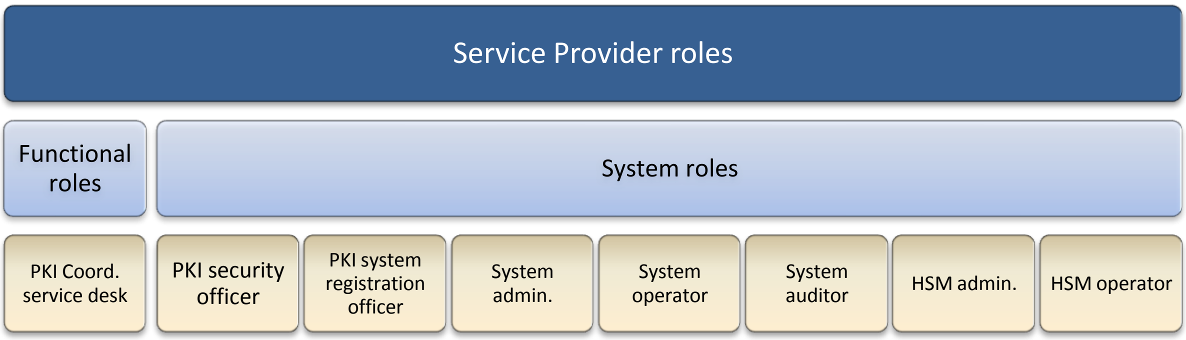
3.1. SERVICE PROVIDER ROLES

The ESCB-PKI Service Provider is responsible for:

- Guaranteeing that the data for the creation and verification of the digital signature is complementary;
- Providing information to the certificate subscriber, free of charge, either in written form or by email about her responsibilities;
- Not keeping nor copying subscriber information other that necessary for the provision of the service;
- Keeping an up-to-date directory containing the certificates and information about their current expiration and revocation status;
- Employing qualified personnel experienced in the certification services offered;
- Revoking certificates and publishing this fact through CRLs in an elapsed time no longer than that stated by the SLA, once the revocation request has been received;
- Facilitating access by electronic means to the latest version of the CPS and the CPs;
- Abiding by all personal data protection laws that apply;
- Issuing all requested certificates according to the norms and procedures established in the CPS and subsequent CPs;
- In general, abiding by all the obligations imposed by the CPS, CPs and applicable legislation.

This section describes the roles required to operate the ESCB-PKI services by the Service Provider, namely Banco de España (BdE). The roles are grouped in two categories:

- Roles for operating the PKI system;
- Roles for operating the Hardware Security Modules.



3.1.1. FUNCTIONAL ROLES

ESCB PKI Coordinating Service Desk

The ESCB-PKI Coordinating Service Desk ensures the 2nd tier of support.

3.1.1. PKI SYSTEM ROLES

The PKI system is the core infrastructure required to provide public key services such as key pair generation, public key certificate issuance and life cycle management, CRL generation, issuance of OCSP tokens, etc.

The roles required to operate the PKI System are:

PKI Security Officers

They have overall responsibility for administering the implementation of the security policies and practices. For-eyes principle is required to change relevant policies of the PKI (e.g. modify or add certificate profiles).

PKI System Registration Officers

They are responsible for the approval of certificate generation, revocation and suspension, using the Registration Authority services for this purpose. They are in charge of managing certificates for the PKI subsystems (CA, RA, VA and KA).

System Administrators

They are authorised to install, configure and maintain the PKI system, but have no access to security-related information.

System Operators

They are responsible for operating the PKI system on a day-to-day basis. They are authorised to perform system backup and recovery procedures.

System Auditors

They are authorised to view the PKI system archives and audit logs.

HSM Administrators

They are responsible for carrying out administrative tasks in the HSM hardware.

HSM operators

They participate in the daily operation of the PKI system.

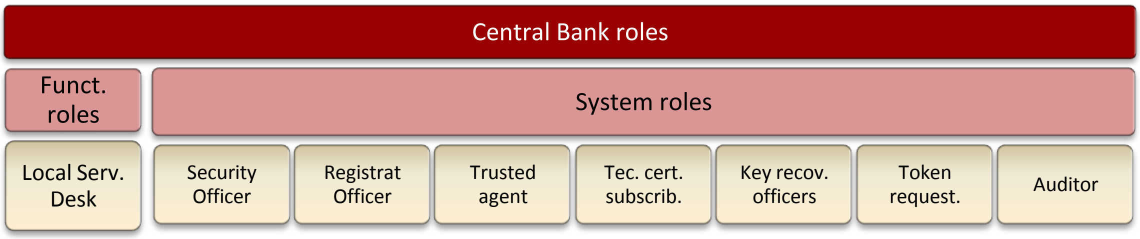
3.2. CUSTOMER ROLES

This section describes the roles that will be delegated to the Central Banks and external organisations. The roles are grouped in two categories:

- Central Bank roles;
- External organisation roles.

3.2.1. CENTRAL BANK ROLES

Roles described below will be available to Central Banks in order to manage certificates and cryptographic tokens.



FUNCTIONAL ROLES

ESCB PKI Local Service Desk

The ESCB-PKI Local Service Desk ensures the 1st tier of support for internal and external users.

PKI SYSTEM ROLES

Security Officer

Responsible of:

- Defining the appropriate configuration settings according to the CB preferences (i.e. Key recovery option);

Registration Officers

Responsible of identifying certificate subscribers, validating the documentation required during the identification process, gathering all the information necessary to issue the public key certificate and finally allowing the user to retrieve the certificate. The following types of RO roles will be available to every Central Bank:

Registration Officers (RO) are in charge of managing digital certificates for their Central Bank internal users (ESCB Users).

Registration Officers for External Organisations (RO4EO) are a particular type of ROs. They are ROs from a Central Bank that are in charge of managing digital certificates for persons and technical accounts that belong to external organisations, typically (but not always) from the same Central Bank's country.

Registration Officer for Technical Components (RO4TC) is a specific type of Registration Officer that is in charge of managing technical certificates by approving or rejecting certification requests that have been carried out by Technical Certificate Subscribers. This role will be used only by those Central Banks that require managing technical certificates.

Registration Officer is responsible for:

- Checking subscriber identity and personal circumstances pursuant to CPS and corresponding CPs;
- Verifying that all information contained in the certificate request is complete and sufficient in compliance with the certificate CP.
- Archiving the documentation

They interact with the PKI Registration Authority subsystem to perform the following operations:

- Generate/download requested certificates;
- Disable/enable remote download feature;
- Suspend/reactivate certificates;
- Revoke certificate.

Trusted Agents

They are authorized to provide Certificate Subscriber face to face identification during the registration process. Trusted Agents will not have automated interfaces with Registration Authority subsystem. This role will be required for those cases where the end user to be registered is not near a Registration Officer.

Technical Certificate Subscriber (TCS)

They are in charge of requesting and retrieving certificates for technical components (e.g. servers, SSL accelerators, applications, etc.). This role will be used only by those Central Banks that require managing technical certificates and it will be typically assigned to technical experts from the IT department.

They interact with the PKI Registration Authority subsystem to perform the following operations:

- Generate/download certificates;
- Suspend certificates.

Key Recovery Officers (KROs)

They participate during the recovery of encryption key pairs from the Key Archive, when the owner of the key pair is not present. This role shall only be required by those Central Banks that request the use of the Key Recovery service.

Cryptographic Token Requestor

They request secure tokens to the ESCB-PKI service provider. The ESCB-PKI will provide Central Banks with cryptographic tokens for their users upon request.

Auditor

They are in charge of verifying that the local ROs perform their tasks in accordance to the rules defined in the CPS and the corresponding CPs.

3.2.1. EXTERNAL ORGANISATION ROLES

The following ESCB-PKI system roles will be available for external organisations.

External organisation roles
System roles
Trusted Agents

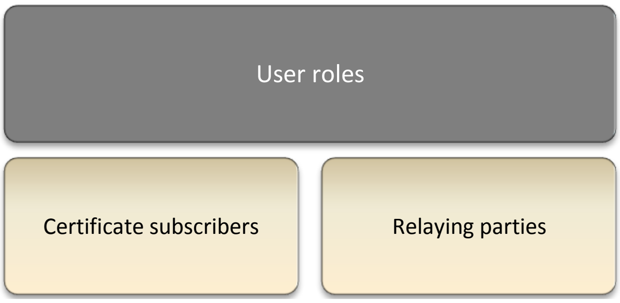
No functional roles will be assigned to external organisations.

Trusted Agents

They are authorized to act as a representative of a Central Bank in providing external Certificate Subscriber face to face identification during the registration process. Trusted Agents will not have automated interfaces with Registration Authority subsystem. It will be up to each Central Bank to decide the legal binding with the trusted agent.

3.3. USER ROLES

This section describes the end user roles, i.e. users without responsibilities in managing certificates for other users.



Certificate subscribers

They are the end users from Central Banks (ESCB users) or external organisations (non-ESCB users) for which a certificate has been issued by the ESCB-PKI. They have the following responsibilities:

- Provide accurate, full and truthful information when filling the application form;
- Inform the ESCB-PKI of any data modification;
- Take the all necessary security measures in order to avoid any loss, disclosure, modification or unauthorised use of the cryptographic card issued;
- Be responsible for the secure custody of the PIN and PUK secret numbers for activation and unlocking the cryptographic card;

- Request the certificate's revocation in case of data application form variation or inaccuracy, or when the private key might be under risk due to, among other causes, loss, theft, or knowledge by third parties of the PIN and/or PUK.

They interact with the PKI Registration Authority subsystem to perform the following operations:

- Generate/download her certificates;
- Suspend her certificates.

Relying parties

They are either individuals or organisations that recognise and rely on a certificate issued by the ESCB-PKI. That is, relying parties understand the linkage between the public key contained in a certificate and the identity of the subscriber, in order to verify the integrity of a digitally signed message, identify the creator of a message or establish confidential communications with the subscriber.
Relying Parties must make use of the information contained in the certificate (such as the certificate policy identifiers) to determine the suitability of the certificate for a particular use.

4. ALLOCATION OF ESCB-PKI ROLES

European System of Central Banks

System Owner: the System Owner of the ESCB-PKI service is the Information Technology Committee (ITC).

Central Banks

Local System Owner: The Local System Owner (LSO) is the ITC representative at each Central Bank.

ESCB-PKI Access Administrators: In compliance with the IAM Security Policy, the LSO will nominate ***ESCB-PKI Access Administrators (AA)*** who is in charge of granting the required application roles to the appropriate users.

External Organisations

Without delegation of Trusted Agents to the external organisation: every user from the external organisation will need to go physically to the Central Bank of the country where the organization is settled for face-to-face identification.

With delegation of Trusted Agents to the external organisation: in this case, the Central Bank where the external organisation is located will delegate the user identification functionality to a Trusted Agent from the external organisation. The Trusted Agent will not require access to the Registration Authority subsystem but he will only make paper-based work.

The following drawing depicts the role allocation procedure:

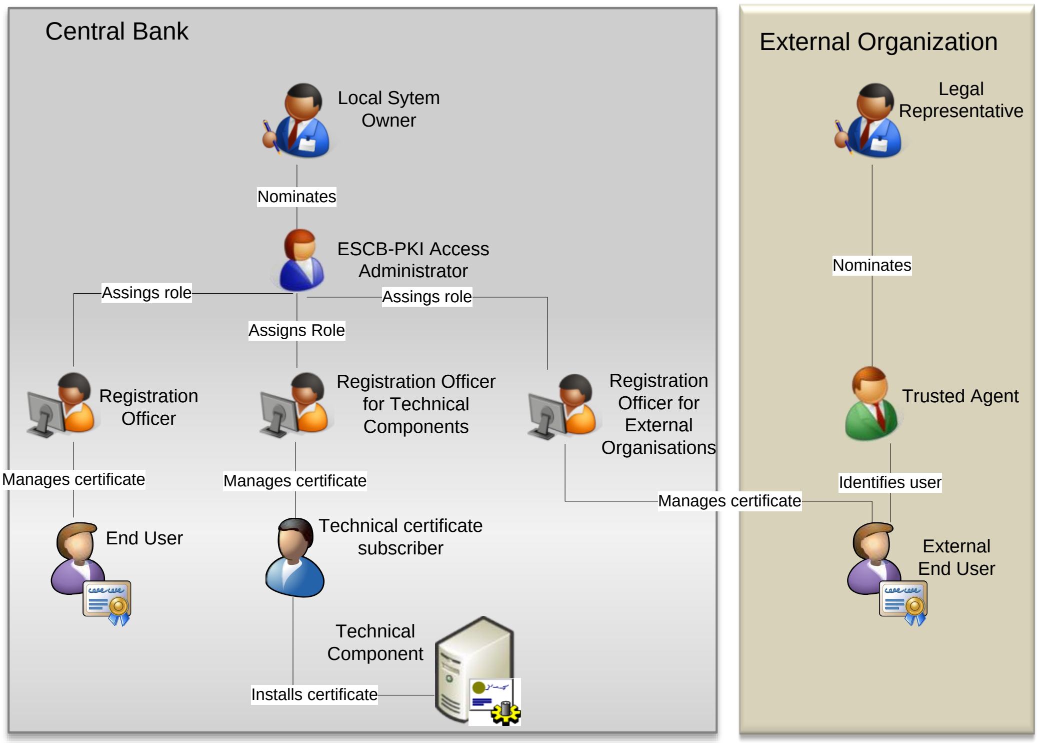


Fig. 1 - Role allocation model

4.1. RULES TO ALLOCATE ESCB-PKI ROLES. SEGREGATION OF ROLES

The following rules must be followed:

- **Registration Officer** is incompatible with **Key Recovery Officer;**
- **Auditor** is incompatible with any other role;
- **PKI System Security Officer** is incompatible with **PKI System Administrator** (service provider roles);
- **PKI System Auditor** is incompatible with any other role assigned to the service provider;
- The following roles must work under the four eye principle, meaning that to perform their assigned duties two people holding the same role must participate:
  - **Key Recovery Officer;**
  - **PKI System Security Officer** (service provider role);
  - **PKI System HSM administrator** (service provider role).

5. ANNEX.

5.1. SUMMARY OF ROLES AND RESPONSIBILITIES

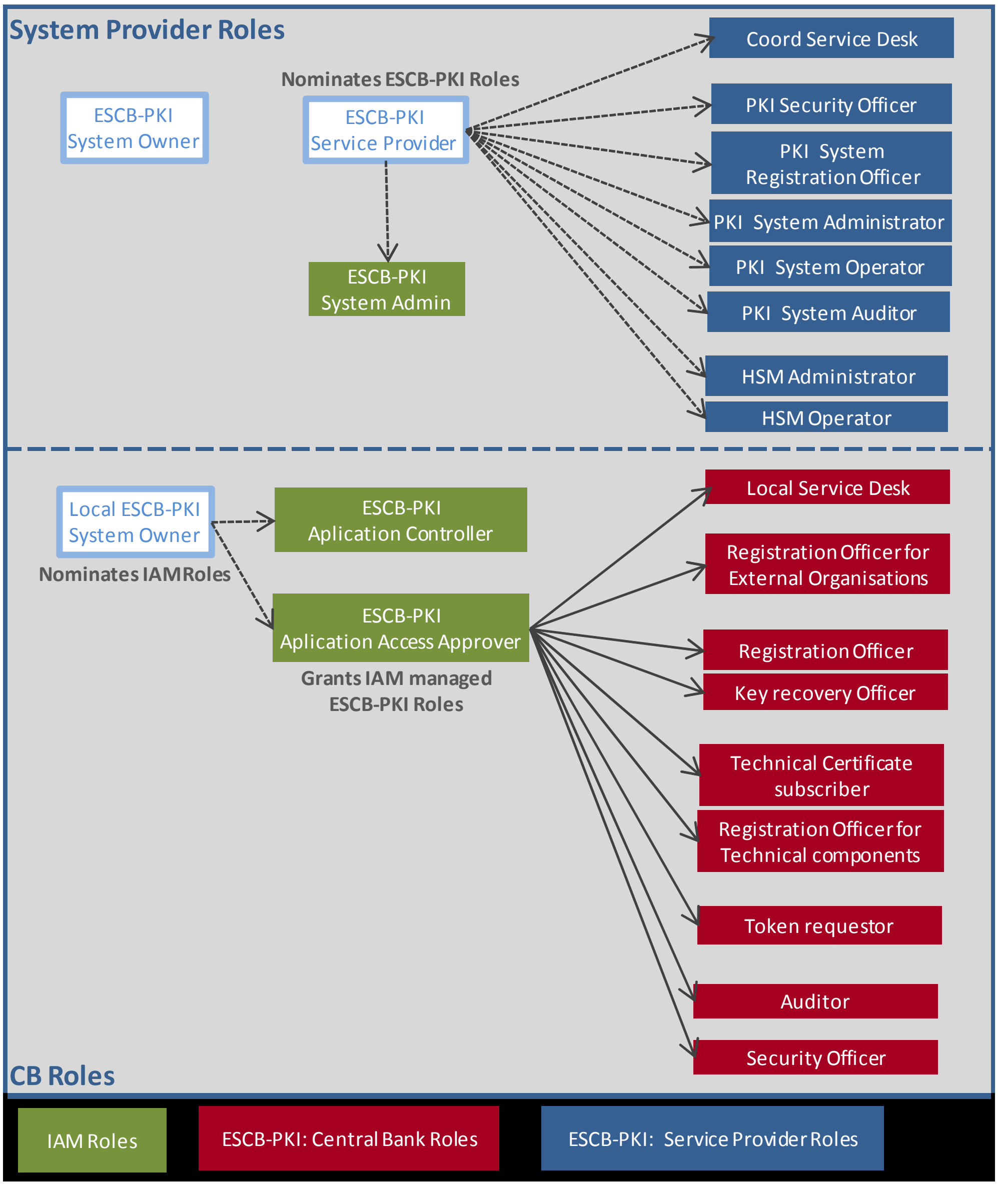

System Provider Roles
Nominates ESCB-PKI Roles
ESCB-PKI System Owner
ESCB-PKI Service Provider
ESCB-PKI System Admin
Coord Service Desk
PKI Security Officer
PKI System Registration Officer
PKI System Administrator
PKI System Operator
PKI System Auditor
HSM Administrator
HSM Operator
Local ESCB-PKI System Owner
Nominates IAM Roles
ESCB-PKI Aplication Controller
ESCB-PKI Aplication Access Approver
Grants IAM managed ESCB-PKI Roles
Local Service Desk
Registration Officer for External Organisations
Registration Officer
Key recovery Officer
Technical Certificate subscriber
Registration Officer for Technical components
Token requestor
Auditor
Security Officer
CB Roles
IAM Roles
ESCB-PKI: Central Bank Roles
ESCB-PKI: Service Provider Roles

Figure 1 - Summary of roles

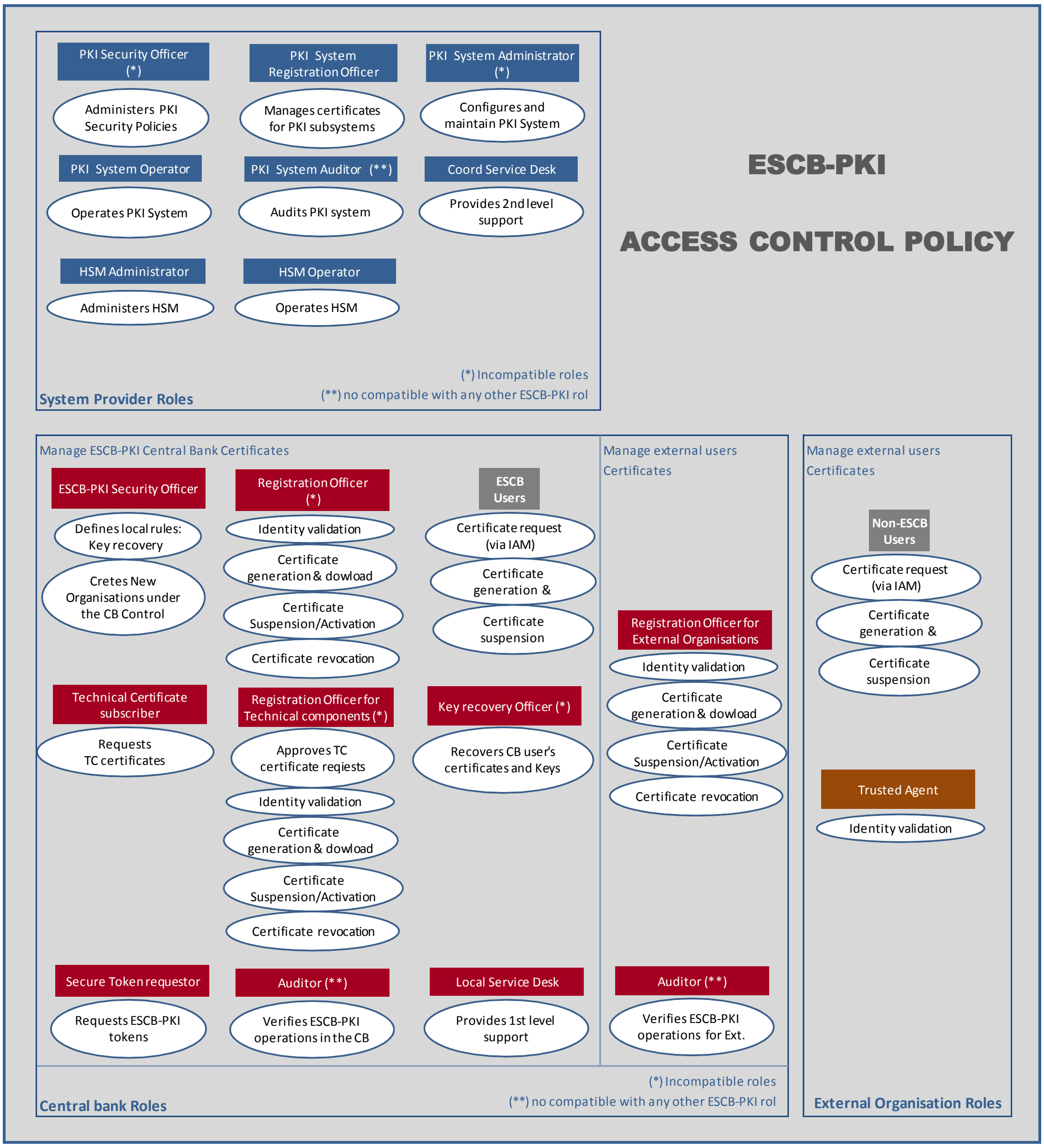

PKI Security Officer (*)
Administers PKI Security Policies
PKI System Registration Officer
Manages certificates for PKI subsystems
PKI System Administrator (*)
Configures and maintain PKI System
PKI System Operator
Operates PKI System
PKI System Auditor (**)
Audits PKI system
Coord Service Desk
Provides 2nd level support
HSM Administrator
Administers HSM
HSM Operator
Operates HSM
(*) Incompatible roles
(**) no compatible with any other ESCB-PKI rol
System Provider Roles
ESCB-PKI
ACCESS CONTROL POLICY
Manage ESCB-PKI Central Bank Certificates
ESCB-PKI Security Officer
Defines local rules: Key recovery
Cretes New Organisations under the CB Control
Registration Officer (*)
Identity validation
Certificate generation & dowload
Certificate Suspension/Activation
Certificate revocation
ESCB Users
Certificate request (via IAM)
Certificate generation &
Certificate suspension
Technical Certificate subscriber
Requests TC certificates
Registration Officer for Technical components (*)
Approves TC certificate reqiests
Identity validation
Certificate generation & dowload
Certificate Suspension/Activation
Certificate revocation
Key recovery Officer (*)
Recovers CB user's certificates and Keys
Secure Token requestor
Requests ESCB-PKI tokens
Auditor (**)
Verifies ESCB-PKI operations in the CB
Local Service Desk
Provides 1st level support
Manage external users Certificates
Registration Officer for External Organisations
Identity validation
Certificate generation & dowload
Certificate Suspension/Activation
Certificate revocation
Auditor (**)
Verifies ESCB-PKI operations for Ext.
(*) Incompatible roles
(**) no compatible with any other ESCB-PKI rol
Central bank Roles
Manage external users Certificates
Non-ESCB Users
Certificate request (via IAM)
Certificate generation &
Certificate suspension
Trusted Agent
Identity validation
External Organisation Roles

Figure 2 - Summary of responsibilities (ACP)

5.2. CERTIFICATE MANAGEMENT FLOW

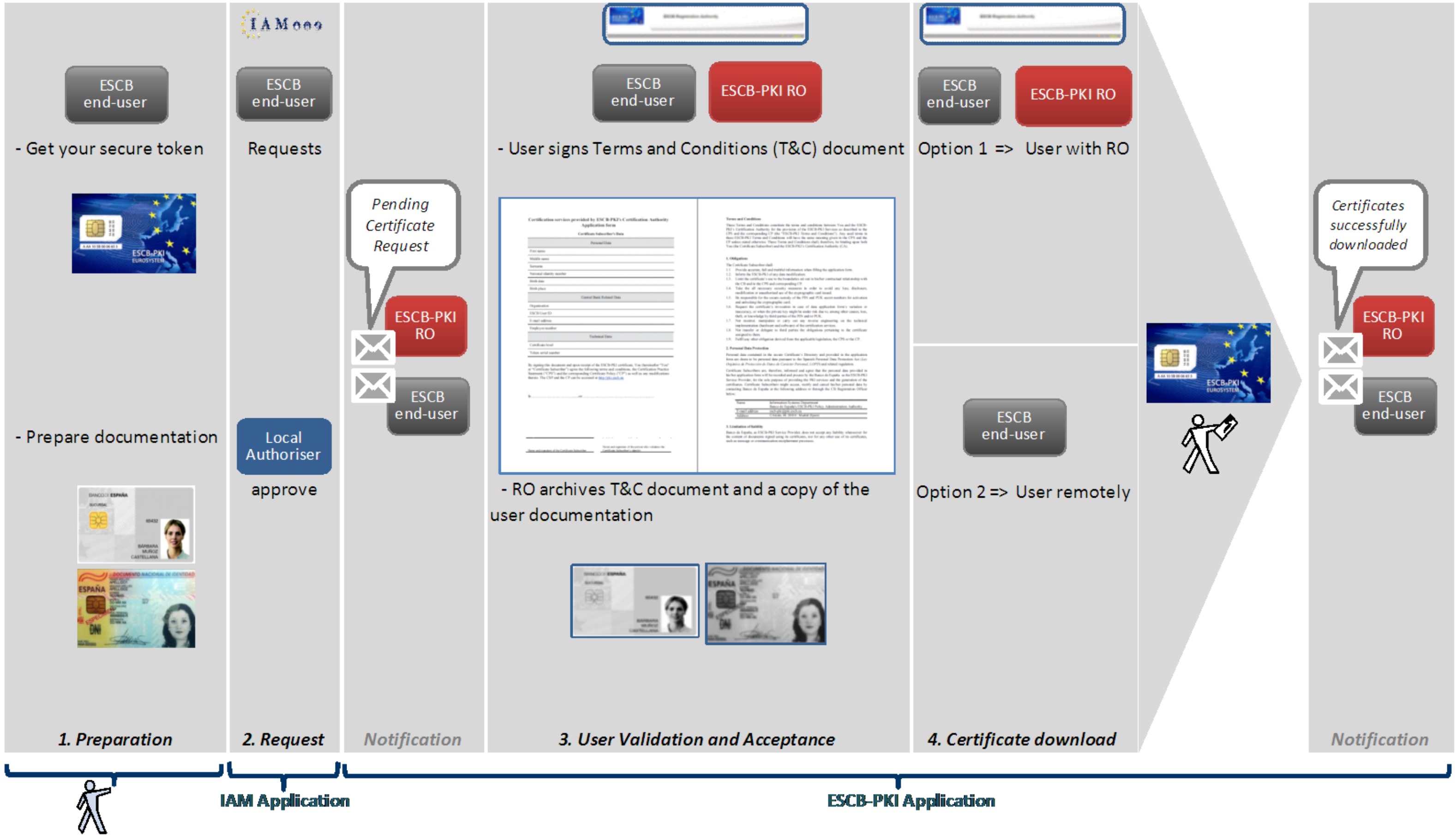


Figure 3 - Advanced certificates request

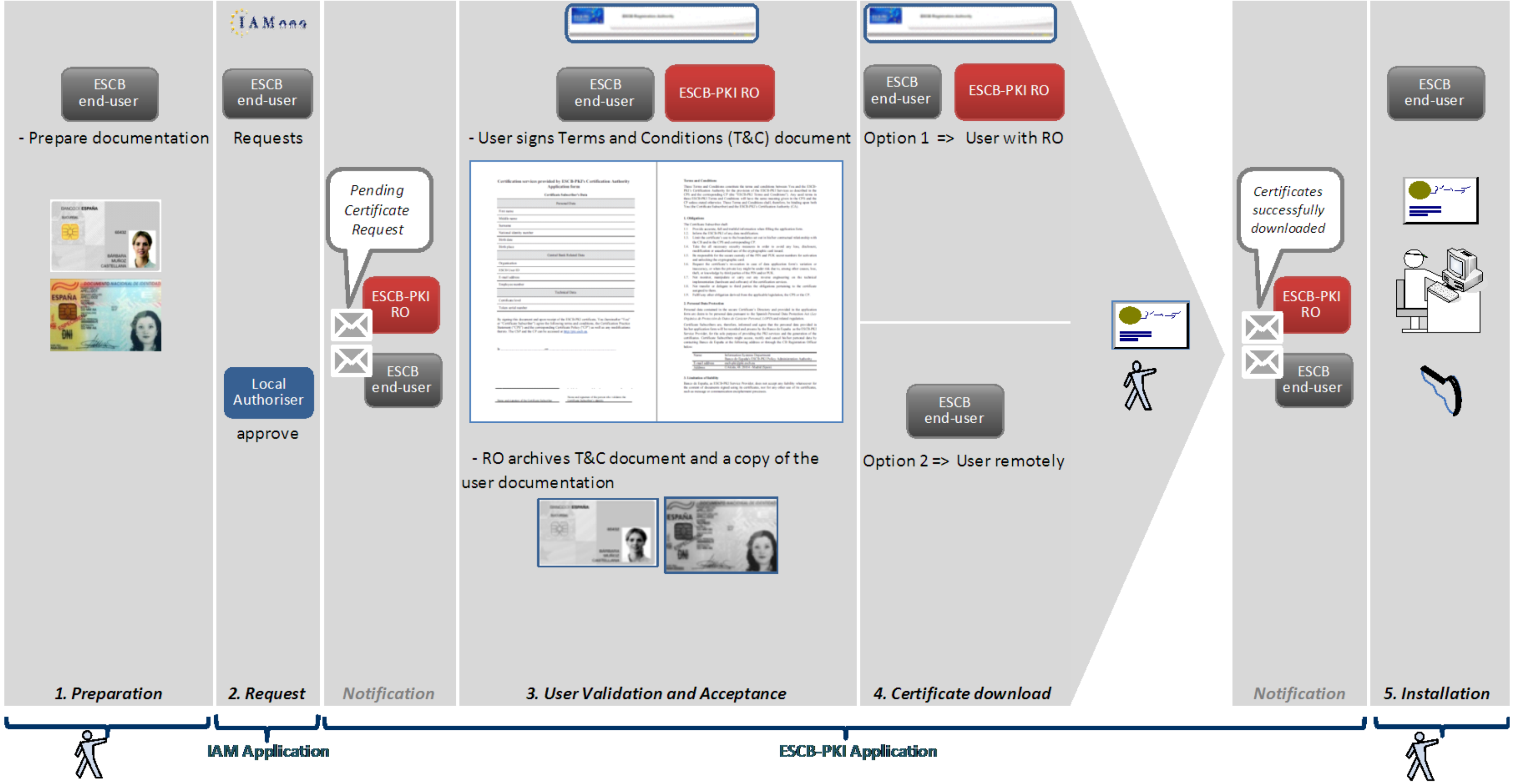


Figure 4 - Standard certificate request

5.2.1. DETAILED PROCEDURES

The last version of this document can be found in the ESCB-PKI Website, along with other ESCB-PKI guides and manuals.

For further information see:

- The ESCB-PKI subscriber's guide;
- The ESCB-PKI registration officer's guide.