available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

The status of National PKIs – A European overview

Dimitrios Patsos [a,*], *Chez Ciechanowicz* [b], *Fred Piper* [b]

[a] *Adacom S.A., Athens 10442, Greece*
[b] *Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK*

Keywords:
National PKI
e-ID
e-passports
e-tax
e-health
e-justice
Digital signatures
Smart cards

ABSTRACT

A series of European Union initiatives and frameworks have been issued during the last years, for the provision of electronic services to individuals, businesses and government organizations. Most of these efforts imply the use of digital certificates for a wide variety of national and transnational transactions. This paper presents the concept of National PKI through a systemic view, compares and contrasts the main inhibitors and enablers, discusses popular use cases, and also examines the European landscape together with open issues.

1. Introduction

Governments around Europe are turning to provide electronic services as a means of social inclusion, effective public administration and better quality of life for their citizens (European Commission, 2010). Electronic services are mainly targeting to effectively and efficiently control tax declaration revenues, provide secure information exchange for travellers, control national and European borders, and reduce administration costs, for EU citizens and residents.

Towards this direction, a large number of initiatives and interoperability frameworks have been introduced to the EU countries. Notable examples include the Secure IdenTity AcrOss BoRders LinKed (STORK) for Electronic Identities (e-ID), the Pan European Public Procurement Office (PEPPOL) for public procurement and the European Patient Smart Open Services (epSOS) for e-health services. Moreover, as a means of providing more effective border control, many countries (such as Belgium, Austria, Norway, and others) have issued electronic passports, adapted to the International Civil Aviation Organization (ICAO) requirements (VeriSign, 2010).

The aforementioned efforts imply the use of digital certificates as the fundamental means for providing authentication, encryption and digital signatures for transactions between citizens, businesses and government agencies. In this context, the concept of National PKI (referred to as NPKI in this paper) is considered by a large number of governments as the *infrastructure* onto which policies, technology and security can be built upon, in order to provide authentication, identity verification, encryption and non-repudiation in electronic services.

An NPKI is constituted by a Root CA operating at a government level, intermediate Certificate Authorities (CAs) and multiple Registration Authorities (RAs) operating at government agency level (those who actually provide the electronic services), and a wide audience of individuals, businesses and organizations that use digital certificates stored in physical tokens (usually smart cards), as shown in Fig. 1.

Typically, an individual (or an organization) applies for a digital certificate to an RA, which – upon successful verification of the individual's identity- authorizes an associated CA to issue a digital certificate to this applicant.

This paper presents the use of NPKI in Europe by examining the main factors that affect its use at a national level, address its current and future uses, present some notable European implementations, and discuss some of the main open issues.

* *Corresponding author.*
E-mail address: dpatsos@gmail.com (D. Patsos).
1363-4127/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2010.10.007

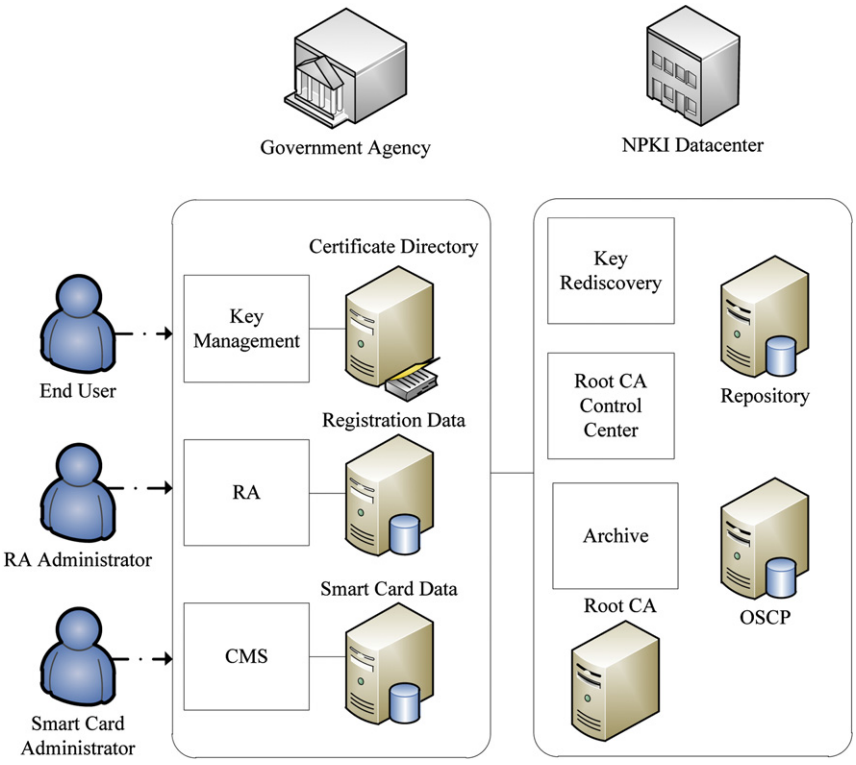

Fig. 1 – A typical NPKI Architecture (Source: VeriSign).

2. A systemic view of national PKI

National PKI is an ecosystem comprised of a diverse set of people, organizations, procedures, constraints, (local, national and international) policies, facilities and technology. Following a systemic approach, we attempt to identify the main aspects of the system, by using the mnemonic CATWOE analysis (Checkland, 1999):

The system *customers* are individuals (citizens or residents), businesses, and government agencies of a country (or a state/region[1]).

The system *actors* are usually the government agencies and/or private companies (such as Ministries, Law Enforcement Agencies, Academic Institutions, Banks, Post Offices, Hospitals, etc.), which provide secure electronic services to *customers*.

An NPKI, from a systemic point of view, collects, processes and stores *customer* data (used as input), and *transforms* this data to data used for authentication, encryption and non-repudiation in electronic services (used as outputs) through complex mathematical equations and IT operations.

As its name implies, an NPKI has a Root CA, which is owned by a country's (or a state's) government. This CA is also referred to as National Root, National CA, or (National) Trusted Root in the associated literature. This National Root must be – literally -public; the *owner* is a government (although there might be some exceptions, such as those discussed in Section 5).

In general, the National Root signs the public keys of other intermediate CAs (government institutions that provide electronic services to *customers*), while it also signs the public keys of individuals and businesses, providing authentication, verification, encryption and non-repudiation services to all parties.

The Government to Government (G2G), Government to Business (G2B) and Government to Citizen (G2C) operations also define the operating *environment* of an NPKI, with respect to the regulatory, technology and privacy issues. Within Europe, there are a number of well-established standards associated with the use of digital certificates, with the *Community framework for electronic signatures* (also known as EU Directive 1999/93), being the most dominant one (European Parliament, 2000). This directive associates electronic signatures with Secure Signature Creation Devices (SSCDs)[2], highlights and enforces users' privacy and defines the criteria for companies and/or organizations that provide certification services (referred to as Certification Service Providers – CSPs). Any European NPKI is highly regulated by this specific directive, and is also tightly coupled with the use of smart cards (as SSCDs).

For simplicity and without real loss of generality, we assume that every certificate is stored on a smart card. When this card is inserted into a (compatible) smart card reader, the holder of this card provides the correct password/PIN thereby authorizing use of the certificate. Note that a smart card may hold more than one certificate associated with one identity.

[1] A common situation in many European countries, where either a state parliament exists or certain regions have some sort of independence.

[2] *A smart card is perhaps the most common form of an SSCD.*