

# **PKI and CA Implementation in the Public and Private Sectors**

**MARIA LOURDES A. YAPTINCHAY**  
Director, E-Commerce Office  
Department of Trade and Industry

**AFP Summit on Enhancing Cyber Security:  
National Cyber Defense Capability Development Conference  
Dusit Thani Hotel, Makati City  
11 March 2010**

# **EXECUTIVE ORDER NO. 810**

## **Certification Scheme for Digital Signatures and Application of Digital Signatures in E-Government Services**

# RATIONALE

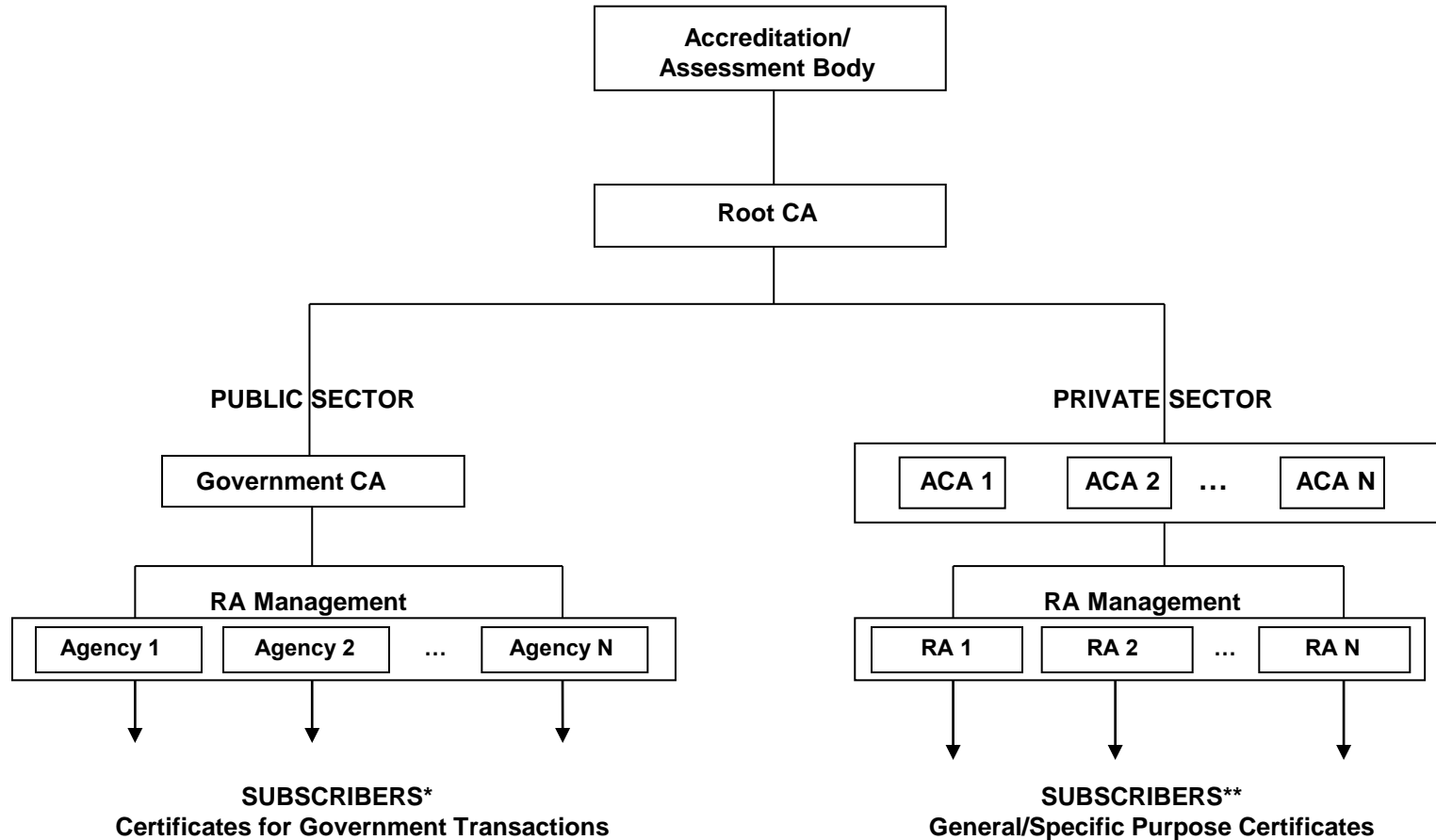
- **Lack of security has been perceived as the main barrier for growth of electronic commerce and wide use of e-government services in the country.**
- **There is a need to provide a secure infrastructure for the exchange of data or information in information and communications technology (ICT) systems.**
- **There is a need to ensure the protection of parties involved in electronic transactions with regard to privacy, confidentiality and content control.**
- **Section 8 of Republic Act No. 8792 or the Electronic Commerce Act of 2000 provides for the legal recognition of electronic signatures and imposing strict requirements before an electronic signature qualifies as a handwritten signature.**

## ***Rationale***



- **By imposing such strict requirements to prove the authenticity, integrity and reliability of electronic signatures, the Electronic Commerce Act validates only electronic signatures, which include, but are not limited to, digital signatures, which are generated through technology that complies with all the requirements enumerated in the Act.**
- **The Rules on Electronic Evidence issued by the Supreme Court in 2001 in accordance with the provisions of the Electronic Commerce Act, defines digital signature as “an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem which generates the signer’s public and private key.**
- **There is a need to institutionalize a certification scheme for digital signatures in the country and designate specific agencies in government which will provide the necessary services to implement the scheme.**

# Framework for the National Certification Scheme for Digital Signatures



*\* Government employees/entities – certificates for all government transactions*

*Non-government individuals/entities – certificates specific to a government transaction (specific purpose certificate)*

*\*\*Private individuals/entities and government employees*

## THE SCHEME:

- The DTI, which is the Accreditation/Assessment Body under this scheme, shall issue the implementing guidelines and the criteria for the accreditation of the Root CA (NCC), the Government CA (NCC), and the private CA. The role of the Root CA is critical to ensure the interoperability of systems among accredited CAs and cross-recognition of certificates within and outside the country.
- The Government CA will issue certificates to government employees and entities which can be used for all government transactions. The Government CA can also issue specific purpose certificates for a specific government transaction to private individuals and entities (e.g. private individual and corporate taxpayers) if they do not have a general purpose certificate issued by a private ACA. In both cases, the Government CA will issue the certificates through a government agency which shall function as RA.
- Government employees have to apply for general or specific purpose certificates from a private ACA for personal transactions with private entities.
- General purpose certificates issued by a private ACA to private individuals and entities can also be used for transactions with government. The private ACA may issue the certificates directly to the subscriber or through a private entity which shall function as RA.

## DEFINITION OF TERMS:

- ***Asymmetric or public cryptosystem*** – a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key for verifying the digital signature.
- ***Accreditation and Assessment Body*** – refers to the body that accredits the CAs and conducts regular assessment of such CAs to ensure compliance to prescribed criteria, guidelines and standards.
- ***Certificate*** – an electronic document issued to support a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair. Certificates issued may be for general use or for specific use only.
- ***Certification Authority (CA)*** – issues digitally-signed public key certificates and attests that the public key embedded in the certificate belongs to the particular subscriber as stated in the certificate. A CA may be involved in a number of administrative tasks such as end-user registration, although these tasks are often delegated to the Registration Authority (RA). The CA may either be a government body or private entity.
- ***Digital Signature*** – refers to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem, such that a person having the initial untransformed document and the signer's public key can accurately determine: (i) whether the transformation was created using the private key that corresponds to the signer's public key; and (ii) whether the initial electronic document had been altered after the transformation was made.

- **Electronic key** – refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.
- **General Purpose Certificate** – a certificate which can be used for all government and private transactions.
- **Registration Authority (RA)** – refers to a third-party used by the CA to perform administrative tasks such as end-user registration. The RA may either be a government agency or private entity performing frontline services.
- **Root CA** – issues and manages certificates to government and private CAs.
- **Specific Purpose Certificate** – a certificate which can only be used for a specific transaction.
- **Subscriber** – an individual or entity applying for and using digital certificates issued by the CA.

# **Guidelines to Implement the National Certification Scheme for Digital Signatures in the Philippines**

- **The Department of Trade and Industry (DTI) will issue the necessary guidelines to implement the National Certification Scheme for Digital Signatures in the Philippines by virtue of its mandate under the Electronic Commerce Act.**

# Designation of Government Agencies and Functions



**Accreditation/Assessment Body – DTI through the Philippine Accreditation Office (PAO)**

**Root CA – National Computer Center (NCC)**

**Government CA – National Computer Center (NCC)**

**RA – government agency with e-government service (e.g. BIR, DBM, NSO, SSS, GSIS, PhilHEALTH, DTI, BOC, DFA, COMELEC, SEC, BSP, GFIs, etc.)**

# Application of Digital Signatures in E-Government Services



**Examples of priority e-government services:**

- **Electronic Filing and Payment System (BIR)**
- **Electronic Procurement (DBM)**
- **Unified Multi-Purpose ID (led by SSS)**
- **Passport Application (DFA)**
- **National Single Window (BOC)**
- **Business Registration (DTI, SEC)**
- **Online banking (GFIs)**
- **Other online services (SSS, GSIS, PhilHEALTH, NSO, etc.)**

# Funding

- **E-government Fund – for e-government services that will immediately apply digital signatures**
- **Regular budget (GAA)**
- **Request additional funds for the PKI project funded by the Korean government through KOICA**

# Application of Digital Signatures in ICT Systems in the Private Sector

- **DTI shall promote the application of digital signatures in ICT systems in the private sector to ensure confidentiality, authenticity, integrity and non-repudiation of electronic transactions with the private sector,**
- **Government agencies or entities exercising supervisory and regulatory functions over private services shall study and identify critical services that use electronic systems which require high levels of security for using and storing personal information and transactions, with the view of strictly requiring the use of digital signatures in such services.**

# Fees

- **NCC, as Root CA and Government CA, will be authorized to charge fees for the issuance of digital certificates guided by the universal concept of user charges, which is to recover at least the full cost of services rendered.**
- **Government RAs will be authorized to charge fees for services rendered. In exceptional cases, however, they may assume the cost of the digital certificates issued to subscribers subject to its contractual arrangement with the Government CA.**
- **The imposition of new fees or increases thereafter shall be subject to the provision of Memorandum Circular No. 137, Series of 2007, and National Economic and Development Authority (NEDA) Circular No. 01-2007.**
- **The costs of digital certificates issued directly by private Accredited CAs (ACAs) or through their respective RAs shall be market-determined, just and reasonable. Private RAs have the option to assume the costs of the certificates issued to subscribers depending on its contractual arrangements with the ACA.**

# Dispute Resolution

- **Cases arising from (1) the accreditation of CAs; (2) the use and issuance of digital certificates; (3) issues necessarily included therein; or (4) issues which include the same, shall be heard and resolved by the respective agencies designated to perform the necessary services in accordance with the rules and regulations to be formulated for such purpose.**

# Transition Period



- **There will be an interim personnel complement to manage and operate the Root CA and Government CA and perform the functions of the respective RAs. Such personnel can either be on detail, reassignment or secondment subject to existing rules of the Civil Service Commission on personnel movements.**
- **DTI and CICT shall determine and recommend to DBM the most appropriate mode of complementing the manpower requirements for the implementation of this Order, such as through the creation of permanent plantilla positions or through contract of services.**
- **In the interim, or until such time that a private ACA becomes operational, NCC shall assume the role of private ACA.**

# **Proposed Rules on Accreditation of Certification Authorities for Digital Signatures**

## **Proposed DTI Department Administrative Order:**

1. Scope
2. Definition of Terms
3. Responsibilities for Accreditation:
  - Philippine Accreditation Office (PAO) under DTI to operate the accreditation scheme
  - Advisory Committee to provide advice to PAO Council
  - Accreditation Evaluation Panel

### Accreditation Criteria:

- Operational
  - Financial
  - Personnel
4. Assessment requirements

## *Proposed Rules on Accreditation ...*

5. Application for Accreditation
6. Renewal of the Accreditation Certificate
7. Grounds for Refusal to Grant or Renew the Accreditation Certificate
8. Terms and Conditions of the Accreditation Certificate and Use of the Accreditation Mark
9. Suspension or Revocation of the Accreditation Certificate
10. Effect of Suspension or Revocation of the Accreditation Certificate
11. Appeal
12. Conduct of Business by the Accredited CA
13. Availability of General Purpose Repository

## *Proposed Rules on Accreditation ...*



14. Specific Purpose Repository
15. Application to Government and Statutory Corporations
16. Disclosure
17. Discontinuation of Operations of Accredited CA
18. Separability Clause
19. Effectivity

Telephone:

897-1243

976-5701/02

E-mail:

[LourdesYaptinchay@dti.gov.ph](mailto:LourdesYaptinchay@dti.gov.ph)

[eco@dti.gov.ph](mailto:eco@dti.gov.ph)