

INSTITUTIONALIZING THE CERTIFICATION SCHEME FOR DIGITAL SIGNATURES AND DIRECTING THE APPLICATION OF DIGITAL SIGNATURES IN E-GOVERNMENT SERVICES

EXECUTIVE ORDER NO. 810, June 15, 2009

Read online (full-text search, related cases, audio case brief): <https://batas.org/library/285250a284f1/>

WHEREAS, 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;

WHEREAS, there is a need to provide a secure infrastructure for the exchange of data or information in information and communications technology (ICT) systems;

WHEREAS, there is a need to ensure the protection of parties involved in electronic transactions with regard to privacy, confidentiality and content control;

WHEREAS, an electronic signature represents the identity of the person attached to or associated with an electronic data message or electronic document, employing any methodology or procedure to authenticate or approve the electronic data message or electronic document;

WHEREAS, SEC. 8 of Republic Act No. 8792 or the Electronic Commerce Act of 2000 provides for the legal recognition of electronic signatures and imposes strict requirements before an electronic signature qualifies as a handwritten signature;

WHEREAS, 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;

WHEREAS, 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 such that a person having the initial untransformed electronic 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”;

WHEREAS, 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;

NOW, THEREFORE, I, GLORIA MACAPAGAL-ARROYO, President of the Republic of the Philippines, by virtue of the power vested upon me by law, do hereby order:

SECTION 1. Adopting a Framework for National Certification Scheme for Digital Signatures. A National Certification Scheme for Digital Signatures in the Philippines, as it appears in Annex A, is hereby adopted.

SEC. 2. Guidelines to Implement the National Certification Scheme for Digital Signatures in the Philippines. The Department of Trade and Industry (DTI) shall, by virtue of its mandate under the Electronic Commerce Act, issue the necessary guidelines to implement the National Certification Scheme for Digital Signatures in the Philippines.

SEC. 3. Designation of Government Agencies and Functions. The following agencies are hereby designated to perform the necessary services under the certification scheme:

a) Root Certification Authority (CA). The National Computer Center (NCC) under the Commission on Information and Communications Technology (CICT) is hereby designated to operate the Root CA. As such, it shall perform the following functions:

- operate the Root CA system;
- issue and manage certificates to accredited government and private CAs;
- develop and prescribe technical standards for digital signatures in collaboration with the Bureau of Product Standards of the Department of Trade and Industry (DTI);
- develop certification technology;
- ensure interoperability of digital certification technology;
- provide technical expertise in the conduct of assessment of CAs when necessary;
- support international cooperation on certification services including mutual recognition and cross-certification;
- resolve disputes involving the issuance and use of digital certificates between concerned parties.

b) Government Certification Authority (CA). The NCC is likewise designated to operate the Government CA. As such, it shall perform the following functions:

- issue certificates for all government transactions to government employees/entities and specific purpose certificates to private individuals/entities;
- publish certificates and Certificate Revocation List (CRL);
- handle revocation requests from the owners of the certificates it has issued.

c) Registration Authority (RA). Government agencies and instrumentalities providing e-government services to its clients shall perform the following functions as RA:

- identify the user and register the user information;
- transmit certificate request to government CA;
- validate certificates from the CA directory server and CRL;
- request revocation of certificates.

d) Accreditation and Assessment Body. The Department of Trade and Industry (DTI), through its Philippine Accreditation Office (PAO), is hereby designated as the accreditation and assessment body for CAs pursuant to its mandate and in accordance with the provisions of the E-Commerce Act. As such, DTI shall perform the following functions:

- Issue the necessary criteria and guidelines for accreditation of CAs to ensure security and interoperability of systems and certificates, as well as compliance with the prescribed standards for digital signatures;

- Accredite CAs, whether government or private, according to the prescribed criteria and guidelines for accreditation;
- Conduct regular assessment of CAs to ensure compliance to existing criteria, guidelines and standards;
- Revoke or suspend the license of a CA for failure to comply with prescribed guidelines and standards;
- Create an Advisory Committee which shall provide direction and advice on the formulation of policies pertaining to the scheme for accreditation and assessment of CAs;
- Create other committees to perform such other functions as may be determined indispensable and necessary to efficiently, effectively and expediently pursue the duties defined under this sub-section.

SEC. 4. Application of Digital Signatures in E-Government Services. All government agencies and instrumentalities providing electronic services to its clients shall require the use of digital signatures in their respective e-government services to ensure confidentiality, authenticity, integrity and non-repudiation of electronic transactions in government. Such projects shall be included in the Information Systems Strategic Plan (ISSP) which government agencies are required to submit to NCC-CICT for approval and endorsement to the Department of Budget and Management (DBM).

The NCC-CICT shall plan, direct and monitor the implementation of this provision in government. Accordingly, it shall assist concerned agencies designated as RA to ensure the smooth implementation of the system.

Within three (3) months from the issuance of this Order, NCC-CICT shall submit to the Office of the President the implementation plan including timetable and required resources to implement this Order. The plan shall identify priority government agencies and instrumentalities and the respective e-government services that will be required to comply within two (2) years from the issuance of this Order. Other government agencies and instrumentalities shall be given three (3) years to comply with this Order.

SEC. 5. Funding and Manpower. To fast-track the implementation of this Order, CICT is hereby directed to prioritize projects of government agencies which are applying for funding under the E-government Fund for projects that will immediately apply the use of digital signatures in their respective e-government services. Such projects remain subject to the requirements of the E-government Fund and must be identified in the agencies' NCC-approved ISSP.

All government agencies and instrumentalities concerned shall submit its manpower and budgetary requirements to the Department of Budget and Management (DBM) to implement this Order. The DBM is hereby directed to ensure that resources will be appropriated in the regular budget of government agencies to implement this Order in consultation with DTI and CICT.

SEC. 6. Application of Digital Signatures in ICT Systems in the Private Sector. In line with its mandate to promote electronic commerce in the country, the 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 are hereby directed to 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.

SEC. 7. Fees. NCC, as Root CA and Government CA, is hereby 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. Similarly, government agencies and instrumentalities performing the functions of RA are authorized to charge fees for services rendered. In exceptional cases, however, government RAs 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.

SEC. 8. 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.

SEC. 9. Transitory Provision. During the initial transitory period after the issuance of the Rules and Regulations to implement this Order, there shall 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.

In the interim, or until such time that a private ACA becomes operational, NCC shall assume the role of private ACA.

SEC. 10. Repealing Clause. All issuances, orders, rules and regulations, or parts thereof, which are inconsistent with the provisions of this Executive Order, are hereby repealed, amended or modified accordingly.

SEC. 11. Effectivity. This Order shall take effect immediately.

Done in the City of Manila this 15th day of June, in the year of Our Lord, Two Thousand and Nine.

(SGD.) GLORIA MACAPAGAL-ARROYO

By the President:

(SGD.) EDUARDO R. ERMITA

Executive Secretary

ABOUT BATAS.ORG

Study smarter at BATAS.org

The Philippine bar review and law-school companion built around how your brain actually remembers.

The complete Philippine law library - free for everyone.

More than 100,000 Supreme Court decisions, Republic Acts, and executive issuances - full-text searchable, browsable by category and year, and always free. No paywall, no login. This PDF came from it.

Audio case-brief lectures.

Any decision becomes a podcast-style lecture - facts, issues, ruling, and doctrine - with read-along highlighting and a hands-free presentation mode. Study while commuting, working out, or resting your eyes.

Bar review built on the science of memory.

Complete, sequenced courses for all eight bar subjects, narrated like podcasts and reinforced with retrieval practice and spaced review - the study techniques with the strongest evidence behind them.

The full law-school curriculum.

One subscription unlocks the entire J.D. curriculum - every subject, every lesson, with your progress tracked down to the paragraph so you can pick up exactly where you left off, on any device.

Mock exams that tell you where you stand.

Timed multiple-choice exams graded instantly, with per-subject score breakdowns and focus suggestions that point you at your weakest topics first.

A study planner that keeps you on pace.

Set your schedule and BATAS tells you every day whether you are on track for bar day - and exactly which lesson to take next.

Start free at <https://batas.org>

The law library is free forever - and your first lesson is one click away.

The text of this document is an official public record and remains in the public domain. Formatting, presentation, and compilation © 2026 batas.org.

Downloaded free from the batas.org Law Library. Share it freely - the library is free for every law student, bar reviewee, and practitioner.