EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate DS - Security
Coordination and Informatics Security

Brussels, 18/02/2011
HR.DS5/GV/ac ARES (2011) 182890
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON CRYPTOGRAPHY AND PUBLIC KEY INFRASTRUCTURE

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 18/02/2011

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.

Commission européenne, L-2920 Luxembourg. Telephone: (352) 43 01-1.

TABLE OF CONTENTS

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

Cryptography is the practice and study of transforming information to make it inaccessible or illegible to unauthorised parties. Within an ICT environment, this is performed through encryption and subsequent decryption of information, using a variety of methods. Encryption is used for a number of different purposes, including protecting the confidentiality of information and guaranteeing the integrity and authenticity of data.

Encryption is a very powerful control, but can also be a very expensive one, and can introduce new risks. In order to guarantee the effectiveness of the encryption process, adequate controls and procedures must be put in place.

3. OBJECTIVES

The objective of this standard is to ensure that encryption is used when appropriate, and that appropriate controls are put in place to ensure that the encryption is effective and does not create new risks.

4. SCOPE

This standard applies to all current or proposed EC systems that use cryptography, including but not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs, smartphones etc.), storage devices, network equipment and media storage (floppy disks, USB devices etc.). The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties in possession of such information.

The standard is applicable to all systems that use cryptography[1], handling both EUCI and non-EUCI, although systems handling EUCI must comply with additional rules[2]. Chapter 8 of this document must be followed in all cases when deciding whether cryptography should be used. If cryptography is used, then the rest of the standard must be followed.

The standard is also applicable to systems and information operated by third parties on behalf of the Commission.

5. THREATS COVERED

Security controls defined in this security standard can reduce the impact of the following threats (their description is in the *Standard on Information Security Risk Management*).

T18 – Remote spying

T19 – Eavesdropping

T20 – Theft of media or documents

T21 – Theft of equipment

T22 – Retrieval of recycled or discarded media

T23 – Disclosure

T24 – Data from untrustworthy sources

T36 – Corruption of data

T41 – Denial of actions

6. TERMINOLOGY

There are many terms used in relation to the subject of cryptography. This section only gives a brief explanation of the main terms that are used in this document.

Asymmetric Encryption: an encryption mechanism using a pair of keys where different keys (usually a Public and a Private Key) are used to encrypt and decrypt a message.

Certificate: an electronic text that is issued by a certification authority (CA) and establishes the credentials of the owner. It contains information such as the common name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and electronic signatures), and the electronic signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

---

[1] At least, where a decision to use cryptography is possible. Cases such as the encryption of passwords by operating systems are not in scope, where it is a functional and non-optional feature of the software or hardware in use.

[2] As mandated by Commission Decision C(2001) 844.

Certificate Policy (CP): the CP is a policy statement for a PKI system that defines and limits the intended use of the certificates so that they are only used for approved purposes for which the assured level of trust is adequate.

Certificate Practice Statement (CPS): in a PKI system, a declaration by the CA of the details of its trustworthy system and the practices it employs in its operations and in support of issuance and management of certificates.

Certificate Revocation List (CRL): a list of the identifiers of certificates that have been revoked.

Certification Authority (CA): an entity that is authorised to create, sign, issue, and revoke electronic certificates.

Cryptanalysis: the process of recovering the Plaintext of an encrypted message without the key.

Ciphertext: the encrypted version of the original Plaintext.

Crypto Authority: the director of the Security Directorate, who is responsible for authorising the use of cryptography within the EC.

Cryptography: the study and practice of transforming information to make it inaccessible or illegible to unauthorised parties.

Decryption: the process of transforming Ciphertext back into Plaintext (the reverse of Encryption).

Electronic Signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Encryption: the process of transforming Plaintext information into Ciphertext using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a Key. The reverse process is known as Decryption.

EUCI: EU Classified Information, i.e. information classified at the levels RESTREINT UE, CONFIDENTIEL UE, SECRET UE or TOP SECRET UE.

Hashing: a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the "message digest" or simply "digest".

Key: a code that is used together with an encryption algorithm to encrypt and/or decrypt information. Keys may be of differing lengths according to the algorithm and option chosen, typically ranging from 64 to 2048 bits. As a general rule, the longer the key, the more secure the encryption but the more processing power is required to perform the encryption / decryption.

Key Escrow: a procedure for storing copies of keys with one or more third parties to enable their recovery in case the operational copy is lost. Keys may be split into

two or more parts, each of which is lodged with a different party to ensure that no single third party possesses the entire key.

Key Management: the set of procedures to be followed for tasks such as key generation, distribution, replacement, storage, recovery and deletion.

Key Recovery: the process of retrieving a lost key, e.g. from a back-up or from Key escrow.

PKI: see Public Key Infrastructure.

Plaintext: the original, unencrypted information.

Private Key: the secret component of a pair of cryptographic keys used for Asymmetric encryption.

Public Key: the publicly disclosable component of a pair of cryptographic keys used for Asymmetric encryption.

Public Key Infrastructure (PKI): a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke certificates.

Registration Authority (RA): an entity that collects and verifies, on behalf of a CA, the Subscribers' identities and other attributes to be included in the electronic certificates. A Registration Authority may not sign or revoke certificates.

Relying Party: A recipient of a certificate who acts in reliance on that certificate and/or any electronic signatures verified using that certificate.

Shared Key: a secret key that is shared between two (or more) parties so that only they can encrypt and decrypt information. See Symmetric encryption.

Steganography: A cryptographic technique whereby information is hidden among other information such that it is not normally detectable. This is often done nowadays by hiding information in media files such as pictures, videos or sound files, through making changes that are imperceptible to a person but which can be decoded using the appropriate software.

Subscriber: a CA Subscriber is an entity (a person or a computer system) whose name, or other information suitable for identification, is included in an electronic certificate issued by a CA.

Symmetric Encryption: an encryption mechanism where the same secret key is used to both encrypt and decrypt the information, and is therefore known by both the sender and the receiver.

Virtual Private Network (VPN): a communication channel passing over a (public) network that is considered to be as secure as a private network due to the packets being encrypted.

7. BACKGROUND INFORMATION

7.1. Introduction

Computer cryptography is a very broad and complex subject, encompassing both the technical and procedural aspects of encryption and decryption. This standard will not attempt to provide a complete overview of this topic, since there are many other resources available for that purpose. Some knowledge of the following areas of encryption may be necessary in order to understand and apply this standard:

- Encryption algorithms
- Symmetric and asymmetric encryption
- Public Key Infrastructure
- Hashing
- Electronic signatures

The information in this section is included only as guidelines (background for the rest of the standard). Rules are given in sections 8 to 9 of this document. Guidelines for PKI implementations are given in section 10.

7.2. Use of Cryptography

Cryptography can be a very effective measure to protect information, particularly when that information is stored on or transmitted through systems or networks that are not controlled by the Commission. Depending on the algorithm and key length chosen, the average time required to break the encryption of information can make this unfeasible (e.g. many years). Due to the constantly increasing power of computers, however, these values are constantly falling and so cryptographic controls must be chosen to take into account the potential computing power available over the lifetime of the information[3].

Although there are many different applications of cryptography, they are all designed to protect one or more of the following properties of information:

- **Confidentiality** by ensuring that unauthorised parties cannot access the plaintext and so understand the information.
- **Integrity** by ensuring that an unauthorised party cannot change the information, due to its being encrypted and therefore inaccessible, or because the unauthorised party would be unable to recreate the encrypted data (or message digest), or by detecting that the data has been tampered with.

[3] In practical terms, this can mean simply choosing a greater key length than is required at present.

- **Authenticity** by demonstrating that the information could only be encrypted by the holder of a private key, based on the principle that the owner of the private key is the only entity (person or computer system) that possesses it.

Integrity and authenticity controls are usually applied through the use of electronic signatures (see below).

Cryptography can be used in many different circumstances, all of which are covered by this standard. Some of the main uses are summarised below.

Passwords are usually stored in encrypted or hashed form within the authenticating system. Where the user can only log on locally, this may be controlled very simply; where the user can log on remotely, more complex processes such as hashing are used to protect passwords passing over networks.

Information held in **databases** may be encrypted to prevent an unauthorised user with direct access to the database from understanding or using it.

Network communications can be secured, either through the use of encrypted protocols where all network communications are encrypted (e.g. for wireless networks or sensitive wired networks), or through the use of encrypted tunnels or **Virtual Private Networks** (VPNs) over untrusted networks.

Electronic mails, messages or transactions may be encrypted and/or digitally signed to guarantee their privacy, integrity and authenticity.

Electronic signatures[4] (also sometimes called **Digital signatures**) are used to guarantee the origin and/or content of a message or other data.

Files stored on computer equipment or media (e.g. back-up tapes, disks or USB memory devices) can be encrypted to protect their confidentiality and/or integrity.

A **Digital Fingerprint** is a hash-value of a document that is used to verify the integrity of a signed electronic document.

Whole disk encryption is an effective way to protect information, particularly on portable end-user devices such as laptop PCs. It is

[4] See also the following documents:

- Directive 1999/93/EC on a Community framework for electronic signatures
- Commission Decision 2004/563/EC, Euratom, regarding electronic and digitised documents
- SEC(2005)1578 Electronic and Digitised Documents – Implementing Rules

This standard does not replace or in any way modify the above documents.

mandated by this standard for all Commission laptop PCs (see section 8.1.1 below).

Web communications may be encrypted, often via HTTPS using SSL or TSL, to guarantee the identity of either party and/or to protect the data transmitted.

Interactive application sessions may be encrypted to protect data in transit from the user's workstation to the application server.

Application-to-application communications can also be encrypted.

File transfers and **remote file services** may be encrypted, usually for confidentiality.

Network printer communications may be encrypted to prevent sensitive information being printed from being intercepted.

Several of these functions are supported by Public Key Infrastructure (PKI) systems, which provide a framework for issuing and using public/private key pairs. This standard therefore contains some specific rules for PKI systems (see section 10).

7.3. Risks of Cryptography

Although cryptography is a powerful security control, improper use can lead to a number of risks, due to either inadequate procedures or malicious use, such as the following.

- Encryption can introduce technical complications such as problems in establishing secure (encrypted) network connections.
- If encryption keys are not adequately protected, there are risks that information may be compromised when it is believed to be intact (e.g. revealed to unauthorised parties, or maliciously altered without this being detected).
- Encryption can also cause effective (temporary or permanent) loss of data, if the information only exists in encrypted form but the key is lost.
- Cryptographic tools could be used for hiding data associated with illegal activities and impeding investigation procedures.
- Encryption of communications (such as e-mails or Internet traffic) can make it impossible to scan for viruses or other threats at the gateways.
- Organisational shortcomings, such as inadequate key management, can undermine the solution.
- Human errors such as violations of basic legal conditions for the use of cryptographic procedures can cause the solution to fail.

- Technical failures, such as weaknesses in cryptographic algorithms, may introduce vulnerabilities.

- Deliberate acts, such as unauthorised use of a crypto module for nefarious purposes, can introduce other vulnerabilities or liabilities.

To avoid these risks, cryptographic solutions and procedures must be designed with great care and forethought.

8. CRYPTOGRAPHIC MEASURES

Policy objective 6.6.1 – Policy on the use of cryptographic measures – Cryptographic measures for the protection of information must be approved in advance and their use will be allowed for certain purposes and under certain conditions. Cryptographic measures must be used in compliance with all relevant agreements, laws and regulations.

8.1. Identifying cryptographic requirements

8.1.1. Introduction

Most of this standard is concerned with the more complex uses of cryptography which are generally more costly and difficult to implement, and involve the greatest potential risks. However, all uses of cryptographic controls must be approved in advance by the Crypto Authority[5].

When they are required, cryptographic controls must be applied systematically and rigorously, with the participation of all relevant stakeholders, including the LISO, system owner, system manager, IT service provider etc.

Cryptographic requirements are initially determined by the data classification. The following sections specify the procedures for EUCI and non-EUCI.

Encryption should be used in particular where EC information leaves Commission premises. Consequently, whole disk encryption is mandatory for all laptop PCs, irrespective of the classification of data held on them, since they are likely to leave the Commission's premises. Encryption of data stores is also highly recommended for other portable devices, where possible[6] and depending on the sensitivity of the data carried.

Where EC information traverses network links that pass outside EC premises, encryption must be used unless a risk assessment shows that it is not necessary.

---

[5] As noted in the Scope section (§4), this excludes minor built-in encryption functions of software where the feature is not optional (such as encryption of passwords).

[6] This is dependent on the technology being available on other portable devices. At the time of writing, it is still emerging and not yet universally available.

8.1.2. Requirements for EUCI

Communications of classified information (EUCI) must be protected by adequate encryption. Cryptographic products used for the protection of EUCI must be selected and implemented according to the rules laid out in the Commission Decision of 29 November 2001 (2001/844/EC, ECSC, Euratom).

The rules in section 9 of this standard apply to cryptographic solutions for EUCI as well as non-EUCI. However, additional rules may be specified by the above mentioned Decision.

8.1.3. Requirements for Non-EUCI

The decision whether to use cryptography must be based on a documented risk assessment and taken by the System Owner in consultation with the LISO and the IRM, and approved before implementation by the Security Directorate (see section 8.3 below).

The risk assessment must also include an evaluation of the particular threats relating to encryption, as outlined in section 7.3 above.

The *Standard on Asset Management* specifies how systems should be classified for Confidentiality, Integrity and Availability. The classifications for Confidentiality and Integrity may be used (where available) to help determine the use of encryption according to the following table.

Table 1: Cryptographic control recommendations by data classification

INTEGRITY / **CONFIDENTIALITY**	STRATEGIC	CRITICAL	MODERATE
LIMITED HIGH	Should be actively considered	Consider for specific functions or purposes	Only in exceptional cases
LIMITED BASIC	Consider for specific functions or purposes	Only in exceptional cases	Not recommended
PUBLIC	Only in exceptional cases	Not recommended	Not recommended

Data classified as LIMITED HIGH (particularly personal data[7]) must be actively considered for encryption. The decision whether to apply

[7] Systems that handle personal data are obligatorily classified as SPECIFIC and so must undergo a risk assessment, where the need to encrypt should be actively considered (see section 3.4.1 of the Implementing Rules for Commission Decision C(2006)3602).

cryptographic controls must be formally documented, and any decision not to encrypt LIMITED HIGH data must be adequately justified.

Consideration of questions such as the following will also help to define whether cryptographic controls are needed and what kind of solution may be required:

- Does the encryption solution encompass more than one system?
- Does the information traverse any (external) networks?
- Does the information leave the physical perimeter of the EC (e.g. on magnetic / optical media)?
- Is the encryption solution used to authenticate monetary (or similarly sensitive) transactions?
- In case of failure, would the encryption solution be difficult and/or costly to recover or replace?
- Will non-Commission[8] staff, organisations or systems use the encryption solution?
- Will non-Commission staff, organisations or systems be issued with keys?

The proposed use of encryption for a system must be documented and approval sought as described below.

The encryption algorithms used in the products proposed must be well established and considered to be secure. The use of unknown algorithms does not provide extra security since they are likely to be less robust and there are sophisticated tools and methods for reverse engineering algorithms.

8.2. Selecting cryptographic products

The Crypto Authority must be contacted in advance whenever cryptographic products are being considered for selection so that it can provide advice and help the requestor to ensure that the product selected will meet the business requirements and comply with this standard. This must be done before the selection, procurement or use of cryptographic products.

Products should be selected that meet the business requirements and risks fully, but which do not impose unnecessary burdens (cost, administration etc.), since this will increase the risk of the product not being used correctly. It is also recommended that products which are already supported by Product Management within the Commission should be reviewed for

[8] Non-Commission staff means any personnel who are not employed, directly or indirectly, by the Commission (i.e. not Commission officials or contractors). This is not a simple yes or no question; issues to be considered in this area include whether the Commission has contracts and/or NDAs with such personnel or organisations, and what level of assurance the Commission has of their true identity.

suitability before considering new products, since extending the use of an existing product may be more cost-effective, simpler to deploy and avoid the need for the approval process. The approval for these products will include conditions of use, and further use of the same product will not require re-approval as long as it is covered by these conditions. In case of doubt, the Crypto Authority will advise whether a new use case requires re-approval.

When writing a call for tender (or similar document) for any product that uses cryptography, the call for tender documentation must stipulate that all cryptographic solutions are subject to prior approval by the Security Directorate, which will be requested after the winning tender has been provisionally selected but before it is formally accepted. The Security Directorate may veto the selected solution for security reasons.

Care must also be taken in selecting products due to potential import, export or usage restrictions on encryption technology, as determined by the National Security Authority of the country of the manufacturer and the country where the products are used (including countries visited, e.g. for products to be used on portable computers). Cryptographic products must comply with national legislation in the countries where they are used.

Where appropriate, external services may be used to provide cryptographic services such as certificates. However, private keys provided by external services may not be used to encrypt standing data belonging to the Commission, since the Commission may not be able to decrypt the data if the key is lost. These services should therefore primarily be considered for cases such as the following:

- the encryption of data communications, where the encrypted data is decrypted upon receipt (e.g. SSL certificates for use in external communications)
- decrypting information sent to the Commission by external parties
- providing electronic signatures that can be verified by external parties

The use of unspecialised end user products[9] for encryption is not recommended by the Security Directorate, since they often contain vulnerabilities that may be easily exploited and cracking tools are readily available for many of these products.

For cryptographic facilities that are part of other products (such as Office software), the Security Directorate will formulate conditions for use during product selection.

[9] This means products such as compression utilities or office software that offer encryption as an additional feature, but where this is an add-on rather than the core feature of the software.

8.3. Obtaining approval

Once a cryptographic product has been selected to fulfil specific requirements, this must be documented and sent to the Crypto Authority in the Security Directorate for approval before the product is implemented[10].

The request for approval must include at least the following items[11]:

- The classification (for integrity and confidentiality) of the data to be protected
- An overview of the system(s) involved in the solution (including external systems where relevant, and with the boundaries clearly denoted)
- A statement of the risks that the solution is intended to reduce
- A description of the proposed solution, explicitly linking it to the risks
- An assessment of the residual risks after the implementation of the solution, including any risks that are introduced or increased by the solution (e.g. risk of losing data if the key is accidentally destroyed)
- An assessment of the risks inherent in the process or systems
- The relevant security operating procedures (SecOps), covering the measures mandated later in this standard
- The cryptographic product name, and the algorithm(s) and key length(s) to be used
- An overview of the types and numbers of the users of the solution, with training needs
- An outline implementation plan
- The names and signatures of the System Owner, the LISO and the IRM to indicate their agreement with the proposed solution.

When a request is received by the Crypto Authority, it will be evaluated for approval. The approval is based upon an evaluation of the solution rather than of the justification or need for cryptography. The main criteria for approval include:

[10] Cf C(2006) 3602 Article 6, paragraph 1: "The use of encrypting technologies by Directorates-General must be approved in advance by the Security Directorate."

[11] In cases where the information is not available, this should be indicated together with an explanation and discussed with the Crypto Authority.

- An evaluation of the fit of the solution to the requirements, and its justification
- Whether a suitable alternative already exists within the Commission
- Whether the solution proposed uses a reputable, good quality cryptographic product and algorithm, and adequate key lengths
- The adequacy of the SecOps
- For products intended to protect EUCI, whether the rules laid out in C(2001) 844 have been followed correctly
- The implementation and documentation of the key recovery process (see also section 9 below)

In all cases, provision must be made for the recovery of keys used in the encryption process. Where the encryption is applied by end users (most commonly for file encryption), this requirement is still valid but the responsibility lies with the users themselves.

9. KEY MANAGEMENT

Policy objective 6.6.2 – Key management – Key management, including recovery and escrow arrangements, must be in place to support the organisation's use of cryptographic techniques.

9.1. General rules

Key management procedures must be documented and implemented for all cryptographic processes. These procedures must cover at least the following.

Key generation

Keys shall be generated by a random process, in a secure environment and in a way that guessing of the keys or successive keys is not feasible, even if some of the preceding keys are known. In particular, key generators must produce random key sequences that are evenly distributed over the entire key space. Alternatively, key generation may be based on values presented by the user, provided that the process assures that user input is random. In any case, key generators must filter out weak keys.

Use of Keys

Each asymmetric cryptographic key should be used for only one purpose, for example for electronic signatures, or encryption of certain files, or encryption of a communication line. This will enable more flexible key management and reduce the impact in case of compromise of a single key.

Symmetric keys may be used for multiple purposes but this should be limited as much as possible.

Use of cryptographic keys shall require the utilisation of user authentication techniques to ensure that keys cannot be used by unauthorised entities.

Key Distribution

When there is a need to exchange cryptographic keys, those keys must be distributed on suitable data media or via communication links that ensure adequate key confidentiality, integrity and authentication.

Key Recovery

Key recovery procedures must imperatively be covered by the SecOps and must be reviewed by the Security Directorate before product approval may be granted.

Key recovery shall be implemented when there is a need to ensure the availability of data stored in encrypted form[12]. The European Commission shall not implement or apply key recovery mechanisms to recover data that are encrypted on-the-fly during transmission over a telecommunication medium.

The other party (or parties) holding a copy of a symmetric key may not be relied upon for its recovery. Key recovery measures must be controlled by the European Commission.

Key escrow may be used for key recovery. In case external suppliers are used to provide key escrow services, all keys must be split and key fragments lodged with at least two separate parties.

The European Commission shall not implement or apply recovery mechanisms to recover keys used for non-repudiation services. In particular, keys used in electronic signatures may not be recovered (instead, a new signature should be issued).

Key recovery may only be performed by officials of the Security Directorate, with the authorisation of the Crypto Authority, or by the relevant LISO, following procedures that protect classified information and personal data[13]. All actions related to key recovery must be recorded and be available for security audits and investigations.

Changing Keys

Changing keys periodically can increase the degree of security in some circumstances. Hence mechanisms for periodic key refreshing shall be considered and specified in the SecOps (if key changes are not appropriate or necessary, this must be stated explicitly).

---

[12] Cf C(2006) 3602 Article 6, Paragraph 2: "Directorates-General shall put in place means of recovering stored data where the necessary decryption key is not available."

[13] Cf C(2006) 3602 Article 6, Paragraph 3.

Key Storage

Cryptographic keys should be stored in such a way that unauthorised users cannot read, modify or delete them. If possible, cryptographic keys should be stored in an encrypted form. The level of protection over the keys should be designed based on the required level of assurance of the cryptographic system.

Making copies of personal (as opposed to shared) private keys used for electronic signatures or non-repudiation is forbidden. For shared keys, there must be a single owner who controls all copies.

Deletion of Keys

Keys that are no longer required must be destroyed. An adequate sanitisation process shall be used when necessary (e.g. when the medium on which the key is stored will be reused). See the *Standard on Sanitisation of Media* for further information on appropriate sanitisation processes.

10. PUBLIC KEY INFRASTRUCTURE (PKI)

10.1. Introduction

PKI is implemented through an information system that uses cryptography. As such, PKI implementations must follow the rules in the previous sections of this standard. However, PKI is subject to specific rules and terminology, and there are additional guidelines for PKI implementations that are described in this section.

This section on PKI is divided into three subsections. The first includes instructions to be followed during the acquisition of a PKI system. The remaining subsections concern the implementation and operation of PKI systems, and include respectively guidelines for system owners and administrators, and guidelines for end users, in order to clarify the responsibilities of each party.

10.2. Acquiring PKI systems

Like any other cryptographic implementation, PKI systems must be approved in advance by the Crypto Authority. When a requirement for PKI has been identified, the Security Directorate should be contacted to establish whether an existing PKI implementation at the Commission could be used instead of acquiring a new system.

Since PKI systems use encryption, the Security Directorate must be contacted for advice and approval on all PKI systems.

10.3. Rules for system owners and administrators

This section outlines the requirements for Commission bodies that own and/or operate PKI systems.

10.3.1. Certificate Policy and Certificate Practice Statement

Each PKI system must have a Certificate Policy (CP) and a Certificate Practice Statement (CPS) that define the rules and practices governing the security policies and controls of the system, and thus establish the level of trust that may be put in the certificates that it issues. The CP and CPS must be made available to all users of the system.

The CPS documents the practices employed in the operations and management of the PKI system. Where the publication of certain practices would harm the security of the system, they may be excluded from the published version of the CPS.

The Crypto Authority may require owners of PKI systems to submit the CP and CPS for review.

10.3.2. Root Certificate

The root certificate is used to sign the other certificates generated by the system, and the reliability of all certificates depends on the trust value of the root certificate. The confidentiality, integrity and availability of the private key that is used to sign the root certificate must therefore be highly protected, and the root certificate must be renewed on a timely basis to ensure the continuous validity of all certificates.

10.3.3. Certificate management

Registration

Naming

CAs shall generate and sign certificates containing names that uniquely identify the Subscribers across the European Commission and any external organisation that may be involved in the operation of the PKI.

Private Key Generation and Transfer

When the computer module that generates the private key is not under the control of the Subscriber, the key, or a computer module containing the key, shall be delivered to the Subscriber via an accountable method, which shall be described in the approved CPS.

Authentication of Subscribers

The Certification Authority (CA) shall ensure correct binding between identity information and public keys by employing authentication procedures specified in the approved CPS.

The CA shall maintain evidence that due diligence was exercised in authenticating the Subscribers by recording the procedures followed for each certificate.

Certificates

A Certificate shall contain the following information:

- Version
- Serial number
- Name or other information that can uniquely identify the Subscriber to whom the certificate is issued
- Attributes that the certificate binds to the Subscriber. These may include items such as:
    - A public key and the identification of the cryptographic algorithms with which the key must be used
    - Access privileges of the Subscriber
    - Membership of the Subscriber to certain groups
- The beginning and end of the period of validity of the certificate
- The identification of the CA issuing the certificate
- The identity code of the certificate; this should uniquely identify the certificate throughout the life time of the CA
- The usage scope of the certificate
- The algorithm used to create the signature

The certificate must include the signature of the CA.

Certificate Revocation

A certificate must be revoked when the binding between the Subscriber and the public key or other attributes mentioned in the certificate (e.g. dates) is no longer valid.

The CA must authenticate each certificate revocation request to the same level as for the issuing of the certificate.

The CA must revoke certificates as soon as possible upon the receipt of an authenticated revocation request or upon an event rendering the certificate invalid. The CPS shall define the maximum delay for revoking a certificate.

Revoked certificates must be included on the CRL until the certificate expiration date.

The Subscriber, or its owner, shall be notified of the revocation of the certificate.

Certificate Revocation Lists (CRLs)

CRLs shall be made available to the target community (e.g. on a website), and a link to the CRL must be included in all certificates. All appropriate measures shall be taken to avoid denial-of-service attacks that may render CRLs unavailable to the Verifiers.

The CRL posting frequency and the maximum delay for posting a new CRL following a certificate revocation shall be defined in the CPS.

The CA shall publish information on how to obtain, verify and use CRLs in such a way that all potential Verifiers can have access to it.

The CRL shall be signed with the private key of the CA. The verifier must be able to verify the integrity and origin of the CRL by checking the electronic signature of the CRL.

Protection and Usage of Private Keys

The private keys of the Subscribers must be protected through suitable security controls against fraudulent use by entities other than their owner.

Private keys used for electronic signatures or non-repudiation services shall be issued only once and remain under the exclusive control of their owner, and may therefore not be recovered.

10.3.4. Confidentiality

All information or data relating to PKI systems must be classified at least as LIMITED HIGH. If the information to be protected by the PKI system (or the keys that it produces) is classified at a higher level, then the PKI system itself and the keys[14] generated must be classified at the same level.

10.4. Rules for end users

Note: wherever the term "end users" is used in this section, it includes both Subscribers and Relying Parties.

End users must only use certificates for the purposes described in the CP. End users may not use certificates for fraudulent or other illegal purposes, or to masquerade as other users. Subscribers must provide full and accurate information when applying for certificates.

Subscribers must ensure that their private keys remain secret. If specific controls are required by the CPS, they must be followed.

Subscribers must inform the CA immediately if any of the following conditions is true:

- identification information in the certificate becomes invalid;

[14] Except the public keys which must be available to other parties.

- attributes defined within the certificate become invalid;
- the private key of the Subscriber has been compromised;
- the Subscriber has violated the policy rules regarding use and handling of certificates and private keys;
- the Subscriber leaves the European Commission or an external organisation that is served by the PKI;

In this case, or if the Subscriber requests it, the certificate will be revoked. The Subscriber may then apply for a new certificate in the normal way.

When a certificate is revoked, the Subscriber must stop using it for signing and/or encrypting information immediately and permanently.

Relying parties must verify that certificates are within their validity dates and do not appear on the CRL.

11. ROLES AND RESPONSIBILITIES

System Owner

The System Owner of the system using encryption shall be responsible for:

a) determining where there is a need to use cryptography;

b) selecting appropriate cryptographic products, bearing in mind existing products that are supported by Product Management;

c) requesting approval for the use of cryptographic products, where required;

d) defining Security Operating Procedures (SecOps) for the use of cryptographic products;

e) ensuring that the products are implemented, used and decommissioned in accordance with the rules of this standard, the SecOps and any additional requirements or restrictions specified by the Crypto Authority;

f) ensuring that cryptographic products are used in compliance with national import, export and usage restrictions.

System Managers

System Managers in charge of operating cryptographic solutions shall be responsible for:

a) managing the operation of the solutions in accordance with the SecOps;

b) monitoring the security of the solution to detect any security incidents;

c) informing the relevant system managers and LISOs of any security incidents that occur;

d) implementing the necessary containment and corrective security measures when a security incident occurs.

e) where relevant, ensuring that IT service providers comply with the SecOps (e.g. through the use of Service Level Agreements).

IT Service Providers

The providers of cryptographic services or products shall be responsible for:

a) implementing and operating the products in accordance with the SecOps

Crypto Authority

The Crypto Authority shall be responsible for:

a) monitoring the advances in technologies related to cryptography including encryption, authentication, electronic signatures and electronic certification services;

b) setting standards and developing guidelines as regards the use of cryptography within the Commission; standards and guidelines shall be reviewed periodically to ensure compliance with technology advancements;

c) assessing the suitability of cryptographic tools, especially as regards their use in systems handling Classified information;

d) approving cryptographic solutions used within the Commission;

e) advising the Commission services in developing and using cryptographic tools;

f) auditing the development and use of cryptographic tools within the Commission and in particular in Critical and Strategic systems;

g) auditing the use of cryptographic tools by Contractors that may affect the security of the Information Systems of the Commission.

LISO

LISOs shall be responsible for:

a) liaison with the Crypto Authority on the use of cryptographic tools and procedures;

b) analysing the needs in terms of using cryptographic tools in their Directorates-General;

c) advising the Directors-General, Directors, Head of Units, and IRMs on the use of cryptography;

d) performing the recovery of encrypted data when necessary and permissible by the rules in this standard.

All Users

All users shall be responsible for using cryptographic tools according to this policy and the applicable system-specific policies.

12. REFERENCES

Commission Decision (2001/844/EC, ECSC, Euratom) of 29/11/2001

Commission Decision C(2006) 3602 of 16/8/2006

Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006

Standard on Asset Management

Standard on Risk Management

Standard on Sanitisation of Media

Commission Decision 2004/563/EC, Euratom, regarding electronic and digitised documents

SEC(2005)1578 Electronic and Digitised Documents – Implementing Rules

13. RELATED DOCUMENTS

International standard ISO/IEC 27001 – Second edition 2005-06-15

International standard ISO/IEC 17799 – Second edition 2005-06-15

Directive 1999/93/EC on a Community framework for electronic signatures

NIST SP 800-21 Implementing Cryptography

RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework