COUNCIL OF THE EUROPEAN UNION

Brussels, 2 August 2013

11660/13

CSCI 38
CSC 63

"I/A" ITEM NOTE

From :	The Council Security Committee
To :	COREPER/Council
Subject :	Information Assurance Security Policy on Public Key Infrastructure

1. The Council Decision on the security rules for protecting EU classified information [1] requires that "when necessary, the Council, on recommendation by the Security Committee, shall approve security policies setting out measures for implementing the provisions of this Decision." (cf. Article 6(1)).

2. The Council Security Committee has agreed to recommend a policy laying down standards for Public Key Infrastructure for the protection of EU classified information (EUCI) on communication and information systems (CIS) in terms of confidentiality, integrity, availability and, where appropriate, authenticity and non-repudiation.

3. Subject to confirmation by COREPER, the Council is invited to approve the attached security policy.

[1] Council Decision 2011/292/EU, OJ L 141 of 27.5.2011, p. 17

This page intentionally left blank

IA Security Policy on Public Key Infrastructure

IASP 2-4

TABLE OF CONTENTS

I PURPOSE AND SCOPE

1. This policy, approved by the Council in accordance with Article 6(1) of the Council Security Rules (hereinafter 'CSR'), lays down standards for protecting EU classified information (EUCI). It constitutes a commitment to help achieve an equivalent level of implementation of the CSR.

2. The purpose of this Policy on Public Key Infrastructure (PKI) is to define how a PKI is to be used for protecting EUCI, in terms of:

   (a) the overall organisation of PKI;

   (b) constraints on how to use PKI with respect to classification level and other parameters;

   (c) the relationship to other EU policies and documents.

3. The Council and General Secretariat of the Council (GSC) will apply this security policy with regard to protection of EUCI in their premises and communication and information systems (CIS).

4. The Member States will act in accordance with national laws and regulations to the effect that the standards laid down in this security policy with regard to protecting EUCI are respected when EUCI is handled in national structures, including in national CIS.

5. EU Agencies and bodies established under Title V, Chapter 2, of the TEU, Europol and Eurojust should use this security policy as a reference for implementing security rules in their own structures.

6. The PKI in this document refers only to a hierarchal infrastructure managing public key certificates[2] used to protect EUCI.

[2] Other types of certificates, e.g. attribute certificates do not come within the scope of this document.

7. This policy does not apply to PKIs used in any product that is the subject of a second party evaluation[3] as defined in CSR[1] Article 10(6).

8. PKI products must also comply with the IA Policy on Cryptography[4].

II INTRODUCTION

9. Electronic communication within a network of actors (which may be "open"[5]) may require the means to prove the authenticity of messages and the means for providing for the non-repudiation of actions.

10. Such means can be provided by a Trusted Third Party that acts as a notary certifying information for other parties. A Trusted Third Party can be achieved technically by the use of asymmetric cryptography in combination with an appropriate infrastructure and organisation together called a PKI.

11. Statements produced by the PKI, which prove the authenticity of the information, are recorded in a form of a certificate. The certificate, which should have a standardized format, is an electronic document valid for a defined period of time. Certificates are requested by subscribers and they are issued for specific subjects (which may be either individuals or systems). The certificate proving the authenticity of a public key is called a public key certificate. Public key certificates can be used by anybody to verify the authenticity of any information produced by the subject of the certificate e.g. other certificates, Certificate Revocation Lists, emails etc.

12. The stakeholders of the PKI are:

(i) Customers

(a) subscribers: the entities who formally apply for a certificate and who provide the information to be authenticated.

---

3 For example self-contained or external PKI used in COMSEC systems.
4 IASP 2[RESTREINT UE/EU RESTRICTED] IA Security Policy on Cryptography. Document 10745/11
5 In an open network, participants may join or leave without a need to generate new keys

(b) subjects: the entities issued the certificates and who make use of them. A subject may be an individual or an IT system.

(c) relying parties: the entities who check the authenticity of the information and who, therefore, validate the certificate.

(ii) Service Providers

(d) Certification Authority(ies): an entity that formally issues certificates to the subscribers and which has a defined liability.

(e) Registration Authority(ies): an entity to which the subscribers' registration process is delegated by the Certification Authority. A Registration Authority is responsible for verifying the information provided by the subscribers.

(f) auditors: an independent body ensuring appropriate transparency of processes performed by the service provider.

III CONTRAINTS IN THE USE OF PKI

13. The decision to use a PKI should be based on the result of a risk management process. Alternative solutions (e.g. key distribution centre) may be selected if justified.

14. The PKI must ensure the appropriate level of quality of the following:

(a) Registration - the process of applying for the certificate, including verification of the information provided by the applicants (subscribers).

(b) Production of a certificate - the process of the physical construction of an electronic document, generation of the key pair and binding the public key to the subject of the certificate.

(c) Storage, publication and delivery - making the certificate available for all authorised service consumers and delivering the certificate to the actor who will use it.

(d) Suspension/withdrawal - invalidation of a certificate based on a request from one or more authorised users.

(e) Revocation of a certificate - making a certificate permanently invalid on request from a user or because it has reached its expiration date.

(f) Renewal - recreation of the certificate linked to the expiry of the validity date of the certificate, but using same information about the subject and the same public key.

(g) Rekey - production of a new certificate for a given subject with a new key pair.

15. A PKI may only manage the certificates supporting the following security services:

(a) identification and authentication of communicating parties;

(b) verification of the source (authenticity) and integrity of a given set of EUCI;

(c) non-repudiation of actions - ensuring that users cannot deny their actions (vis-à-vis other communicating parties or forensic authorities) and that users can prove the occurrence of transactions;

(d) exchange of session keys for EUCI encryption;

(e) confidentiality - only up to a specified classification level;

(f) a time stamping function providing proof that certain data existed before a defined moment in time.

16. The level of assurance and the constraints in the use (in terms of allowed services and classification levels etc) of the public key certificate must be explained in a Certificate Policy document. The certificates issued by a Certification Authority for the end users must refer to the Certificate Policies with which they are compliant[6].

17. The number of Certificate Policies must be strictly limited in number in order to avoid one Certificate Policy per use of a PKI.

18. Provided it does not contradict the IA Security Policy on Cryptography, the PKI (effectively the Certificate Policies) should preferably respect the constraints set by the Directive on a Community framework for e-signature[7] and the list of associated standards[8] concerning qualified signature.

IV OVERALL ORGANISATION OF PKI

19. The PKI should be centralised in one organisational entity. The use of independent, CIS-specific PKIs should be justified by the risk management process.

20. The PKI should consist of at least two organisational tiers (see Figure 1):

    (a) Tier 1: The PKI Management Authority, the audit and accreditation authorities, the Policy Authority and the highest Certification Authority (root CA);

[6] by means of object identifiers and/or pointers referring to the relevant Certificate Policies and/or Certification Practice Statement (see point 34)

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013 , 19/01/2000 P. 0012 - 0020

[8] 2003/511/EC Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products

(b) Tier 2: Lower level Certification Authorities, optionally Registration Authorities, services for end users (e.g. the helpdesk), optionally Policy Certification Authorities. Tier 2 can be omitted if there is a need for only one subordinate Certification Authority.

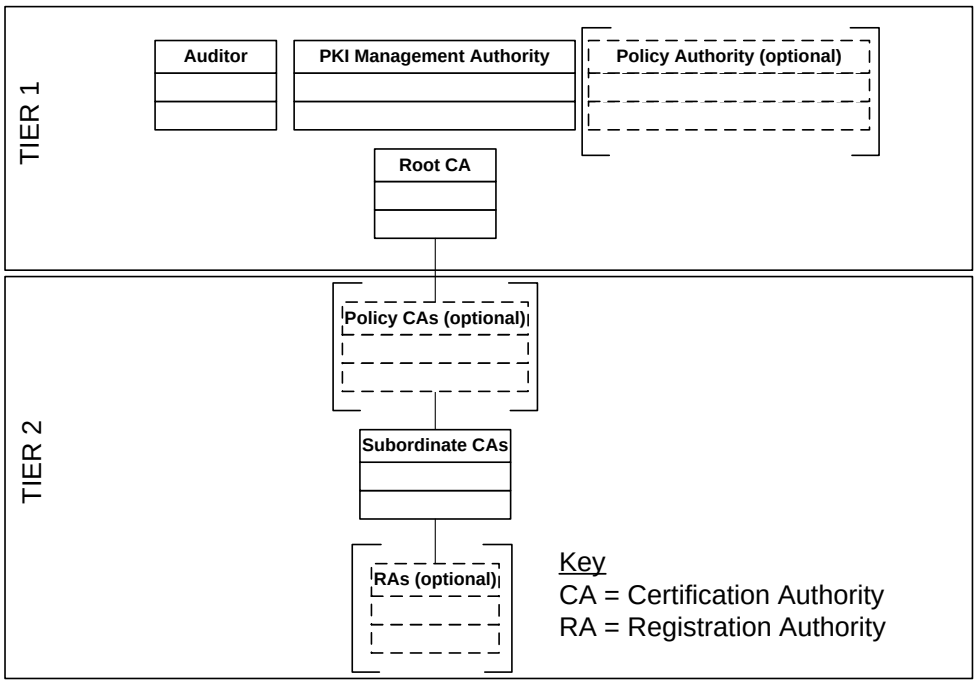

Figure 1 The PKI hierarchy and authorities

21. The responsibility to deploy and manage a PKI must be designated to a PKI Management Authority that can be shared with the role of Sensitive CIS Manager (SCISM) or Information Assurance Operational Authority.

22. The PKI must be regularly audited by an auditor who should be independent from operational roles such as the SCISM and Assurance Operational Authority. The details concerning the extent and frequency of an audit must be described in the relevant Certificate Policy and Certification Practice Statement documents.

23. If justified by its size, the organisation should establish a central Policy Authority that should be responsible for the following tasks:

(a) writing Certificate Policies;

(b) advising other parties on writing their own Certificate Policies;

(c) assessing Certificate Practice Statements ;

(d) assessing external Certificate Policies and Certification Practice Statements when deciding about cross-certification;

(e) maintaining a central registry of existing CAs and their compatibility with existing Certificate Policies;

(f) advising on the use of a particular CA.

24. There should preferably be one or very few central CAs, called root CAs, dedicated to signing certificates for the subordinate CAs.

25. Second level CAs (subordinate CA on Figure 1) should be created to support specific purpose certificates for end users and consequently a specific set of Certificate Policies, for example: server authentication for R-UE/EU-R CIS.

26. The PKI may designate intermediate CAs (Policy Certification Authorities[9]). Such authorities must then support one Certificate Policy each, and may not issue certificates for subscribers other than subordinate CAs (issuing CAs).

27. The CAs subordinate to the Policy Certification Authorities may impose additional constraints on the use of the certificates it issues (e.g. excluding certain uses such as server authentication or signature).

[9] The concept introduced in RFC1422, since replaced by more flexible Certificate Policies

28. The registration and verification of the information provided by subscribers may be delegated to a Registration Authority.

29. Key generation is a strategic decision for the organisation managing PKI. The conditions and responsibilities for the key generation and storage must be described in the respective Certificate Policy.

V DOCUMENTS GOVERNING PKI

30. PKI is subject to accreditation in accordance with the relevant EU security policies and guidelines, specifically the IA Security Policy on Cryptography.

31. Further details for the implementation of this policy, as well as more detailed constraints will be laid down in IA security guidelines on PKI.

32. The format of the certificates must comply with the X.509 standard[10].

33. The details concerning limitations on the use of a particular certificate must be described in the Certificate Policy document(s). Reference to this must be indicated in the certificate in accordance with the Public Key Infrastructure Certificate Policy and Certification Practices Framework[11].

34. The details describing the functioning of a particular CA or RA must be described in the Certificate Practice Statement document according to the Public Key Infrastructure Certificate Policy and Certification Practices Framework. The Certificate Practice Statement must show how the authority complies with the requirements set in the Certificate Policies.

[10] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[11] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

DEFINITIONS

Accreditation	The process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures has been implemented;
(Security)Assurance	Quantitative grounds for confidence that an entity meets its security objectives
(Security)Assurance Level	Discrete value of assurance. In the context of Crypto Policy and cryptographic products there are only two levels - approved (which is expressed by putting a product on the list of products) or not approved (which is demonstrated by the fact product is not placed on the list).
Authentication	The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization.
Authenticity	The guarantee that information is genuine and from *bona fide* sources
Availability	The property of being accessible and usable upon request by an authorised entity.
Certificate	An electronic attestation signed electronically by Certification Authority.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.
Certification Practice Statement (CPS)	A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

Certificate user	See "Relying party" below
Communication and information system (CIS)	Any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. See Article 10(2) of CSR.
Confidentiality	The property that information is not disclosed to unauthorised individuals, entities or processes;
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 of that data
EU classified information (EUCI)	Any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States. See Article 2(1) of CSR
Identification	The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems
Integrity	The property of safeguarding the accuracy and completeness of information and assets;
Non-repudiation	The ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

Public-key certificate (PKC)	An electronic data that binds a public key held by an entity (such as person, organization, account, device, or site) to a set of information that identifies the entity associated with use of the corresponding private key. In most cases involving identity certificates.
Registration authority (RA)	An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying party	A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. The terms "certificate user" and "relying party" can be used interchangeably.
Risk	The potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact.
Subject (Certificate Subject)	The entity whose public key or other attributes are attested by the certificate.
Subscriber (Certificate Subscriber)	The entity that subscribes to the certification authority for the issuance of certificates