Certification Policies
Certification Practice Statement
&
Common Criteria

UNIVERSITÉ Grenoble Alpes

Jean-Guillaume Dumas

Certification policy

- The basis of trust between unrelated entities
- Not a formal contract, but a set of rules for the PKI and the certificate holders
- A framework that constraints a PKI implementation
- A way of giving advice to Relying Parties

- Should describe:
  1. What is the community served ?
  2. What are the rules for identifying Subjects ? (registration)
  3. What is a certificate for ? (encryption, authentication, signature, …)
  4. What is in a certificate ?
  5. What constraints are there on operation of the CA and RA ?
  6. What must be done in case something goes wrong ? (revocation, recovery & continuation plan)

- Reference: [RFC 3647]
  - X.509 Public Key Infrastructure Certificate Policy & Certification Practice Statement Framework

Certification Policy

	Certification Policy
Issuer	Policy Management Authority (could be the CA)
Goal	Describe what is expected from the PKI; needs in terms of trust services, see [RFC 2527].
Usage	Technical & Legal document for audits & exceptional/legal needs Defines applicability and services.
Audience	Both technical employees and external users At a technical level among legal operations, audits and security.

Terms & Conditions

	Subject	User
Issuer	Management	Management
Goal	Describe in simple terms the different possible usage and restrictions applicable to certificates	Describe in simple terms the different possible usage and restrictions applicable to certificates
Usage	Allow final users to clearly understand the limits and conditions of certificate usage	Allow final users to clearly understand the limits and conditions of certificate usage
Audience	Clients of the PKI services	Receiver of a transaction request allowed by the PKI

Contractual terms

	Internal	External
Issuer	Management	Management
Goal	Describe the relations between entities within an organizational unit using a PKI	Describe the relations between entities within an organizational unit using a PKI
Usage	Definition of a context of operations Set up of measurable criteria for the definition of a successful relation	Definition of a context of operations Set up of measurable criteria for the definition of a successful relation
Audience	Technical, legal & audit employees of the different internal entities (e.g. IT, management, security, audit, etc.).	Technical, legal & audit employees of the different external entities (service providers, participants).

Certification Practice Statement

	Certification Practice Statement
Issuer	CA
Goal	Describe how a PKI is managed in order to attain its prescribed goals (in terms of trust services) as specified in the Certification Policy, the T&C or any contractual terms.
Usage	Document the technical, organizational or management controls applied to the CA environment.
Audience	Technical employees implementing the CA or any exceptional needs.

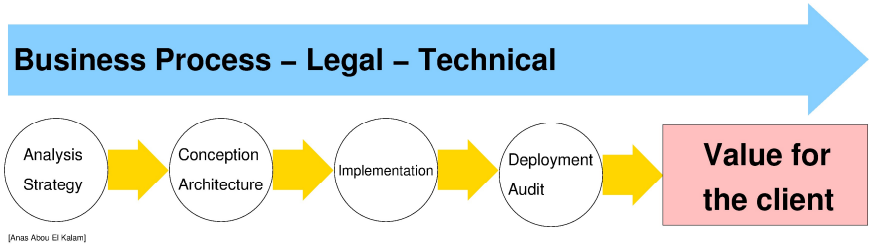
Certificate Practice statement [RFC3647]

1. Introduction (general presentation of the CA, kind of users, machines, networks, services, certificate usage, applications, contacts, etc.).
2. Repository publication responsibility.
3. Identification & Authentication (I&A) (Naming, registration, validation, I&A for revocation or renewal requests, key modifications, etc.).
4. Certificate lifecyle needs.
5. Service, management, and operational commands (physical security checks, audits, logs, archive, Recovery and continuation plan, CA or RA failure, etc.).
6. Technical security checks (generation & installation of key pairs, private key protection, timestamping, etc.).
7. Certificates, CRL and OCSP profiles.
8. Audits.
9. Legal and financial aspects.

Information flow between PC, CPS and T&C

Certification policy	Certification Practice Statement	Terms & conditions
Certificates will be verified each time they are used. Validation receipts will be made in ***nn*** minutes …	Validation will be done via an OCSP maintained in a secure place.	We will check the validity of certificates each time it is used.
Registration will be done by the ***xyz*** RA and will require presentation of 2 id documents.	RA will communicate with the CA via a secure channel using the ***abc*** cipher, each request will be signed, …	To obtain a certificate we will ask you two name and residence proofs (bills, bank statements, driving license, etc.) …
Certificates will be valid for ***nn*** months.	CA will revoke and re-emit certificates every ***nn*** months using existing keys and automatically renew and notify users.	We will provide updated certificates every ***nn*** months.

Deployment of a PKI



Common Criteria: iso 15408

- Goals
  - Common Criteria provide a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation
  - TOE : Target Of Evaluation (product or part of the product to evaluate)
- 7 predefined assurance level (EAL1 to EAL7)
  - Higher is the level, higher is the assurance that the IT product implements correctly and efficiently its security functionalities
- International recognition
  - MRA : Mutual Recognition Agreement
  - 10 countries in Europe
  - 26 countries in the world
  - Recognition applies to EAL1 to EAL4+

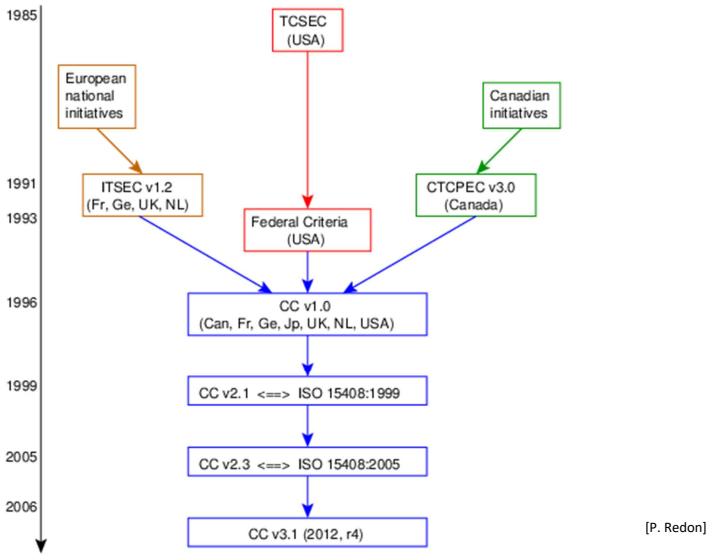
CC overview

- Requirements are provided within 2 documents
  - Functional requirements (known as CC Part 2)
    - A security requirements set where developers can pick up security functional requirements (SFR) their product will have to meet
  - Assurance requirements (known as CC Part 3)
    - A security requirements set where developers will find security assurance requirements (SAR) the product, its documentation or the product's developement team will have to meet
- Vocabulary
  - TOE : Target Of Evaluation (product or part of the product to evaluate)
  - ST : Security Target (security specification and justification of a specific product; also define the evaluation level the product will have to meet)
  - PP : Protection Profile (security specification and justification of a category of products such as firewalls, encryption devices, banking smartcards, …)
  - EAL : Evaluation Assurance Level (predefined set of assurance requirements (EAL1 to EAL7)

Evaluation Assurance Levels

- EAL1: Functionally tested
- EAL2: Structurally tested
- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested, and reviewed
- EAL5: Semiformally designed and tested
- EAL6: Semiformally verified design and tested
- EAL7: Formally verified design and tested

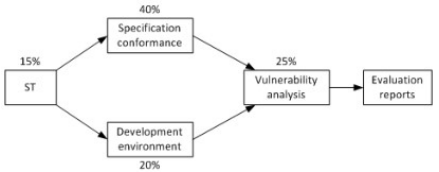
CC history



[P. Redon]

Security evaluation

- In France, performed e.g. by a CESTI
- Performed on hardware and/or software
- Deliverables from the IT product developer
  - Security target
  - Specification & design documentation
  - Test documentation
  - …



- Deliverables from the CESTI
  - Evaluation reports
  - In particular, the product architecture analysis (ADV_ARC) and the vulnerability analysis (AVA_VAN)

Référentiel général de sécurité

- Ordonnance n°2005-1516 (8 décembre 2005)
  - About electronic transactions between users and the “Autorités Administratives” (AA), and between AAs
  - Article 9.I requires the creation of a RGS
- RGS defines a set of requirements for specific services, in regards to a needed security level
  - 4 services
    - Authentication of a user and authentication of a server
    - Digital signature
    - Confidentiality
    - Timestamping
  - 3 security levels for these services: *, **, ***
  - product qualification
  - Certificate Service Provider (CSP) qualification
  - Certificate validation
- RGS main document is completed with appendices

RGS appendices

- About services
- About certification policies
  - CP frameworks for CSP issuing certificates in support to the defined services
- About certificate profile
- About Time parameters
- About cryptography
  - Cryptography mechanisms
  - Key management
- About authentication mechanism

RGS Qualified Cert. Serv. Prov.

- PSCo: Prestataires de Service de Confiance
  - PSCE: Prestataire de Service de Certification Electronique
  - PSHE: Prestataire de Service d'Horodatage Electronique

- PSCo qualification scheme
  - LSTI is the only third party authorised to deliver qualification to PSCo according to the RGS

- A RGS 3 star-level (***) qualified PSCE for the digital signature service is implicitly qualified according to the French arrêté du 26 juillet 2004 (about digital signature)