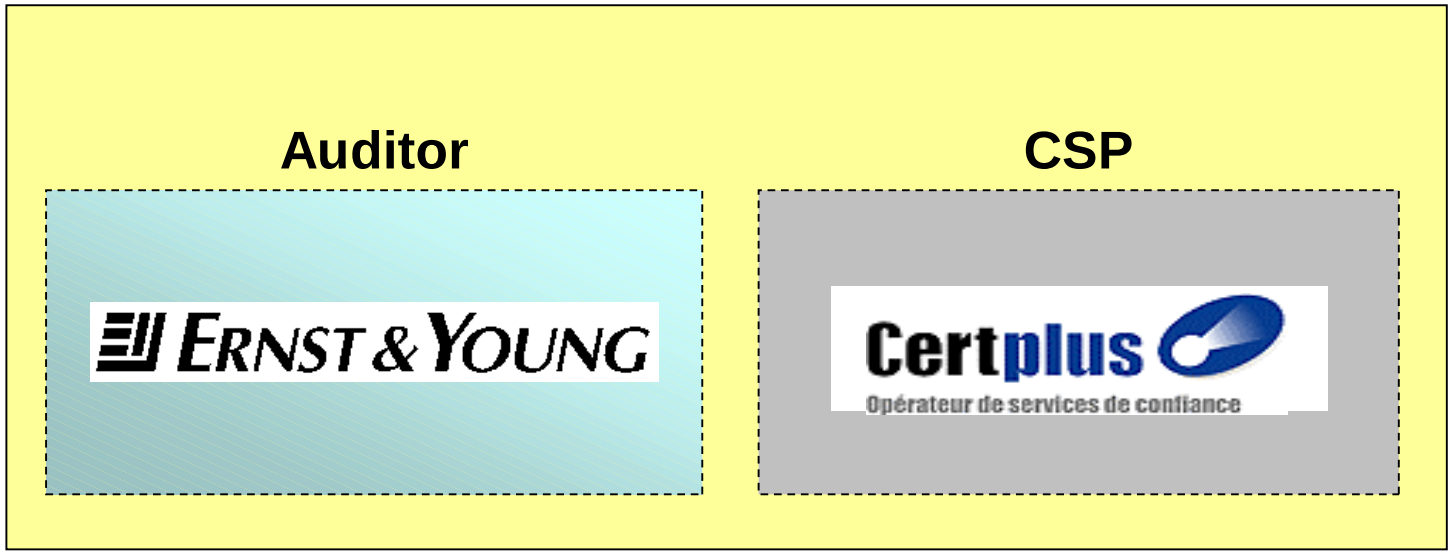
Assessment of Certification Service Providers: The e-Qual project

Lionel Vodzislawsky
Ernst & Young Audit France
Technology & Security Risk Services

E-Qual

Evaluation and Qualification of CSPs



MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Behind the word "qualification"

EC directive, article 3 :

- "…Member States may introduce or maintain voluntary ACCREDITATION schemes …"
- "… Member States shall ensure the establishment of an appropriate system that ALLOWS FOR SUPERVISION of CSP which are established on its territory and ISSUE QUALIFIED CERTIFICATE TO THE PUBLIC."

France (decree 30/03/2001)

- ~~Accreditation~~ ➔ QUALIFICATION
- QUALIFICATION ➔ Presumes CSP compliance to "qualified certificate issuing requirements" (FR Décret – article 6 / EC Annexes I&II)

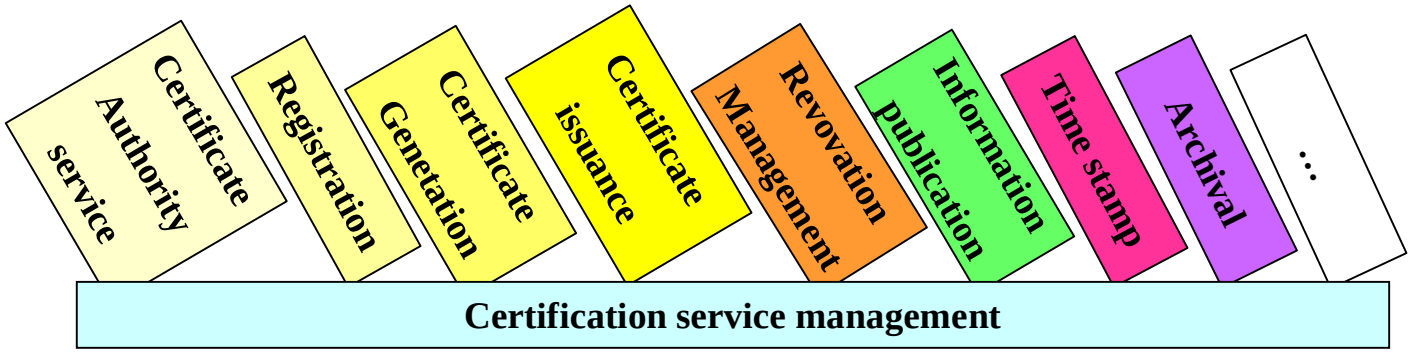
Signature process reliability presumed

What is a CSP?

EC directive, article 2 :

- "Certificate-Service-Provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;
- FR decree : "equivalent" definition

E-QUAL



Aim and perimeter of the project

Propose an efficient, viable (technically and economically) and flexible scheme for the assessment and qualification of CSP

- Focus on keys and certificates life cycle management and related functions
- Address qualified certificates and certificates issuance to the public (signature, authentication, encryption), including legal aspects
- Test the proposed approach through a tentative qualification process
- Uses EESSI and IETF standards documentation as well as Member States conclusions on the subject
- Does not address SCD & SSCD certification, algorithm and key length issues

Base documentation

Regulatory documents

- EC Directive, French implementation

EESSI documents

- TS 101456, CWA 14167-1, TS 101862, CWA 14172 -1 -2 –3

CA Trust / X9.79

tScheme

- Organisation, profiles

ISO / IETF

- ISO17799, (new)RFC2527

Proposed approach

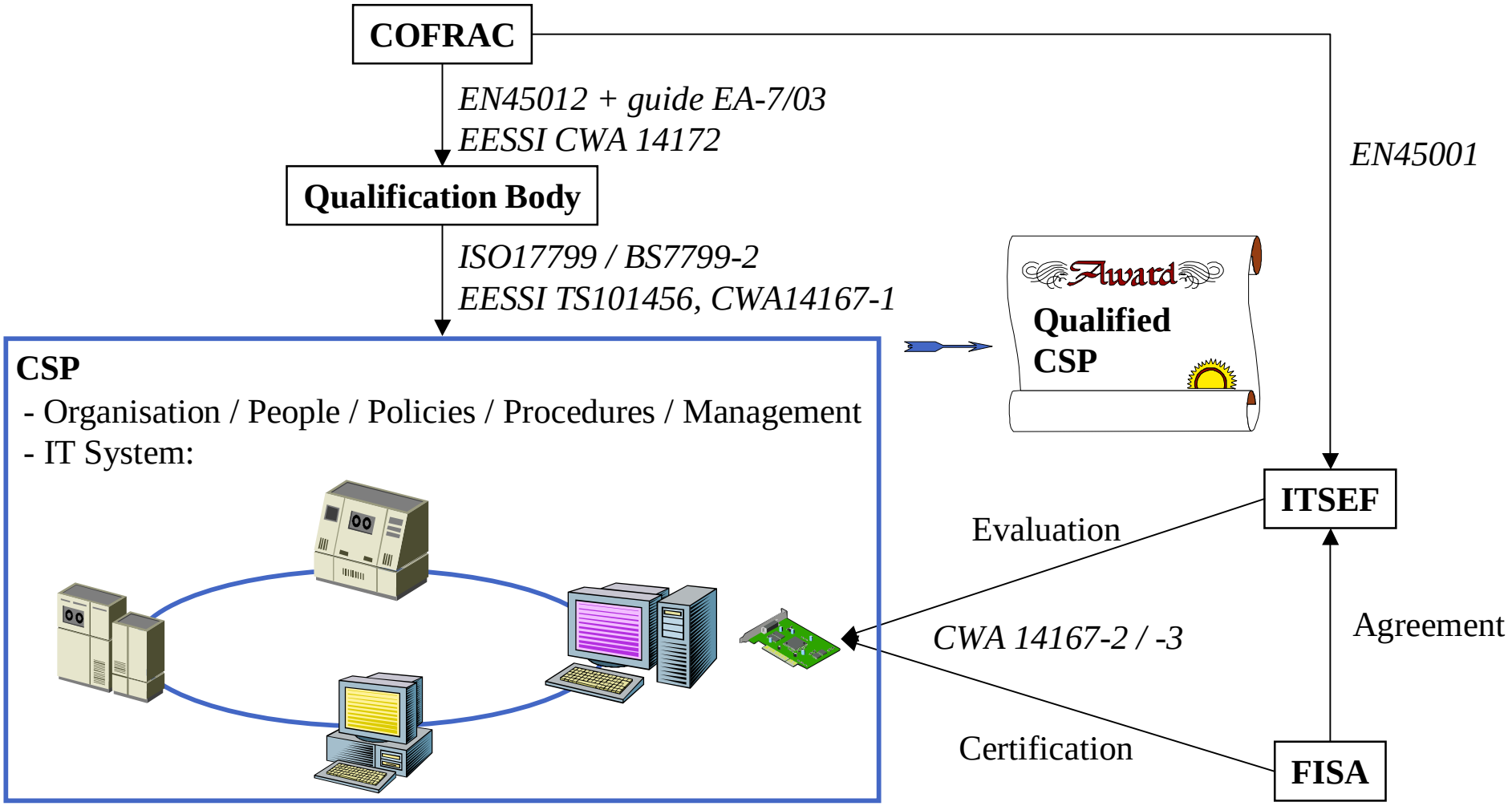
A scheme with a large scope

- The scheme shall not be limited to CSP issuing Qualified Certificates
- It should cover at least all Trusted Third Parties activities

The qualification scheme can be based on a global scheme for evaluation / certification of Information Security Management Systems

- ISO 17799 / BS7799-2

The French approach - General diagram



ERNST & YOUNG
Quality In Everything We Do

Accreditation

Accreditation of Qualification Bodies (QB) against EN45012

- Complemented by the EA guidelines EA-7/03 (ISMS)
- With a verification of the competencies towards the TTP activities that the QB wants to be able to certify (CWA 14172 –2 & -3)

A QB already accredited for ISMS certification has only to demonstrate its competencies

- ☞ Mutualisation of the investments for the QB
- ☞ Reduction of the costs for the clients of the QB (CSP)

CSP requirements (1)

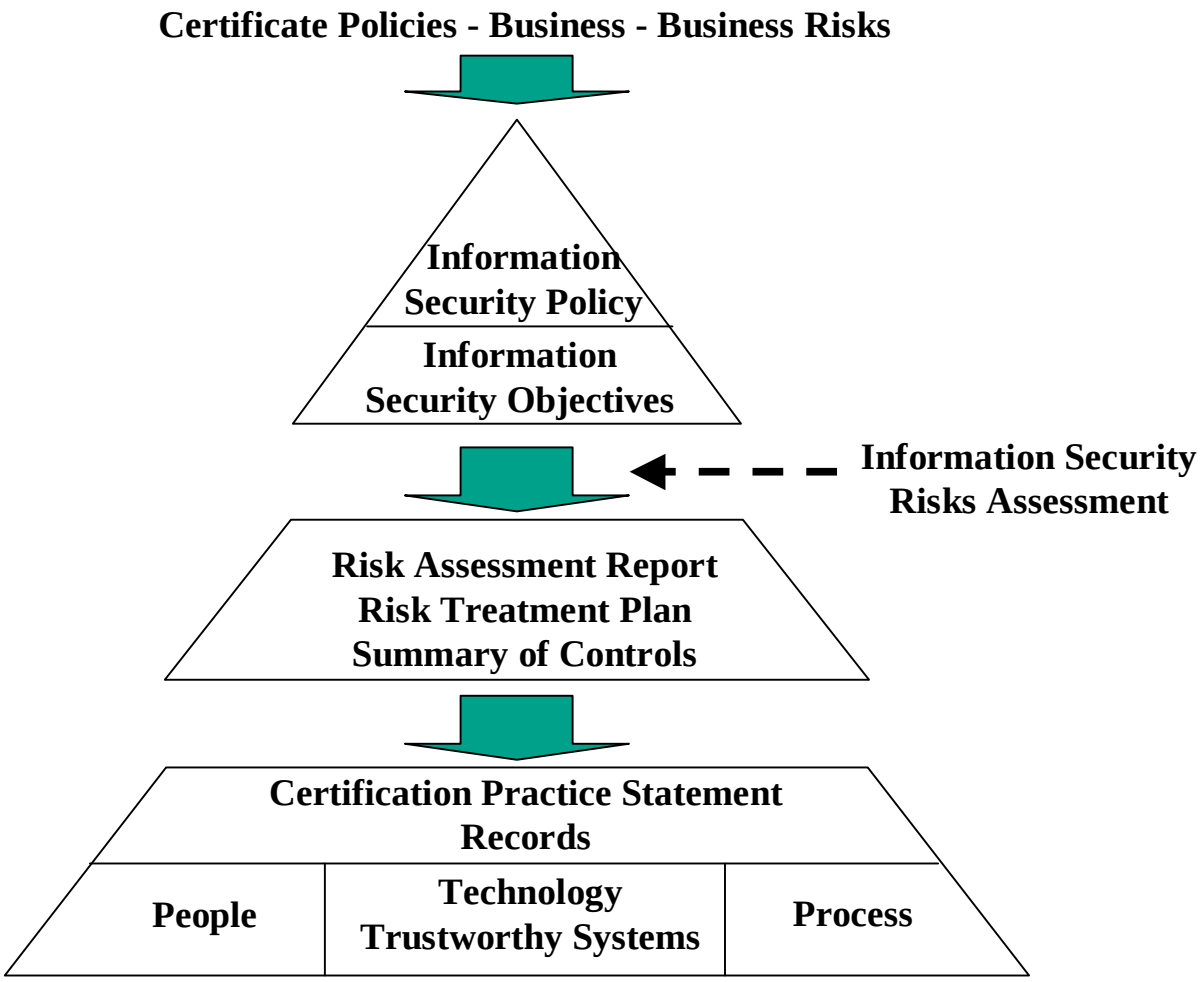
CSP has to put in place an ISMS

- ISO17799 / BS7799-2
- Additional and specific control objectives and controls linked to the CSP activities (TS 101456, X9.79)

CSP has to use Trustworthy Systems

- Which fulfil the requirements of CWA 14167-1 and 14167-2/-3 (crypto modules) (FIPS 140-1 L3?)
- One of the specific control objectives that has to be included in the ISMS

CSP requirements (2)



Qualification

Evaluation / certification of the CSP's ISMS

- Compliant with BS7799-2 (risk assessment, risk treatment plan, selection of controls)
- Compliant with additional control objectives and controls from the appropriate standards (TS101456 for Qualified Certificates, CWA 14167-1, …)

Conformity of the output products to the appropriate standards

- TS101862 for Qualified Certificates

Conclusion

The E-Qual project is still going on

The proposed approach is entirely based on international recognised standards

- The most possible, generic standards: BS7799-2, EA-7/03
- Where necessary, complemented by specific standards: TS101456, TS101862, CWA 14167-1

We think it is the best way

- To set up a viable scheme
- To pave the way for international mutual recognition

For more information

Lionel Vodzislawsky
Senior Manager
+33 (0)5 62 15 43 32
lionel.vodzislawsky@ernst-young.fr

Technology and Security Risks Services

For more information, browse www.ey.com