

FIR DIG *Consultants*

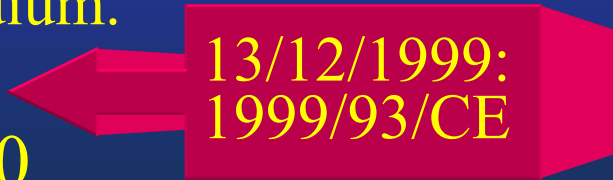
Progetto EESSI
Stato e prospettive

Franco RUGGIERI

f.ruggieri@flashnet.it

Origini dell'EESSI

- In risposta ad una richiesta della Commissione Europea lo European Information and Communications Technology Standards Board (ICTSB) lanciò la European Electronic Signature Standardization Initiative (EESSI), varata il 24 febbraio 1999 a Bruxelles.
- Phase 1: individuare le aree carenti di standard
 - il Final Report del 20/7/1999 ne individuava 20 con tre livelli di priorità: Urgent, High, Medium.
- Phase 2: partì a gennaio 2000
- Phase 3: partì a gennaio 2001
- Lunedì scorso 21/1/2002 è partita la fase 4.

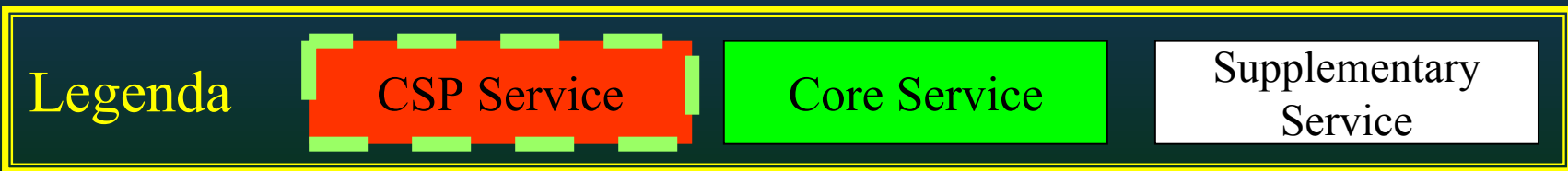
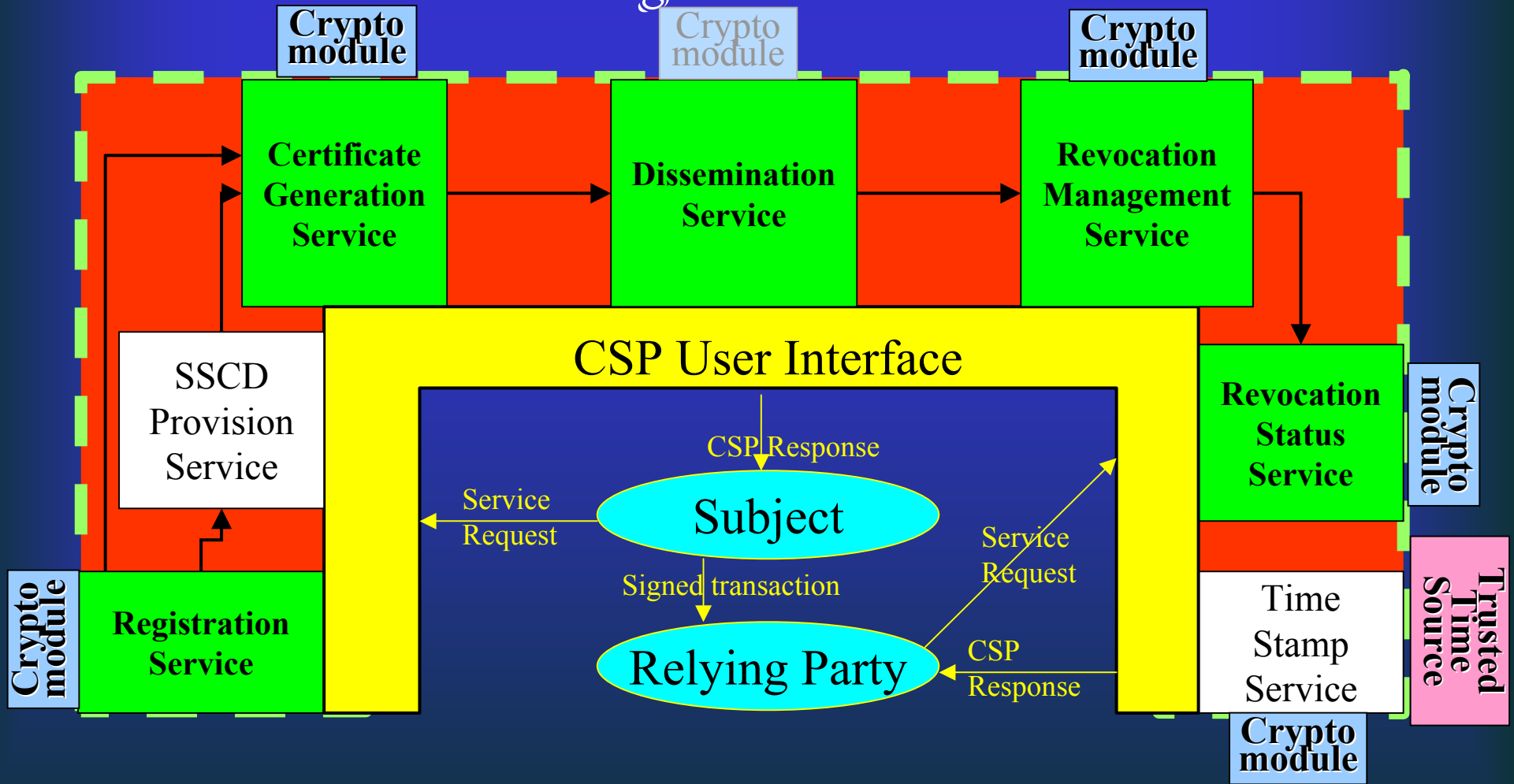


13/12/1999:
1999/93/CE

Riferimenti

- ETSI:
<http://www.etsi.org/sec/el-sign.htm>
- CEN:
<http://www.cenorm.be/iss/workshop/e-sign>
- EESSI:
<http://www.ict.etsi.org/eessi/EESSI-homepage.htm>

Architettura generale di un CSP

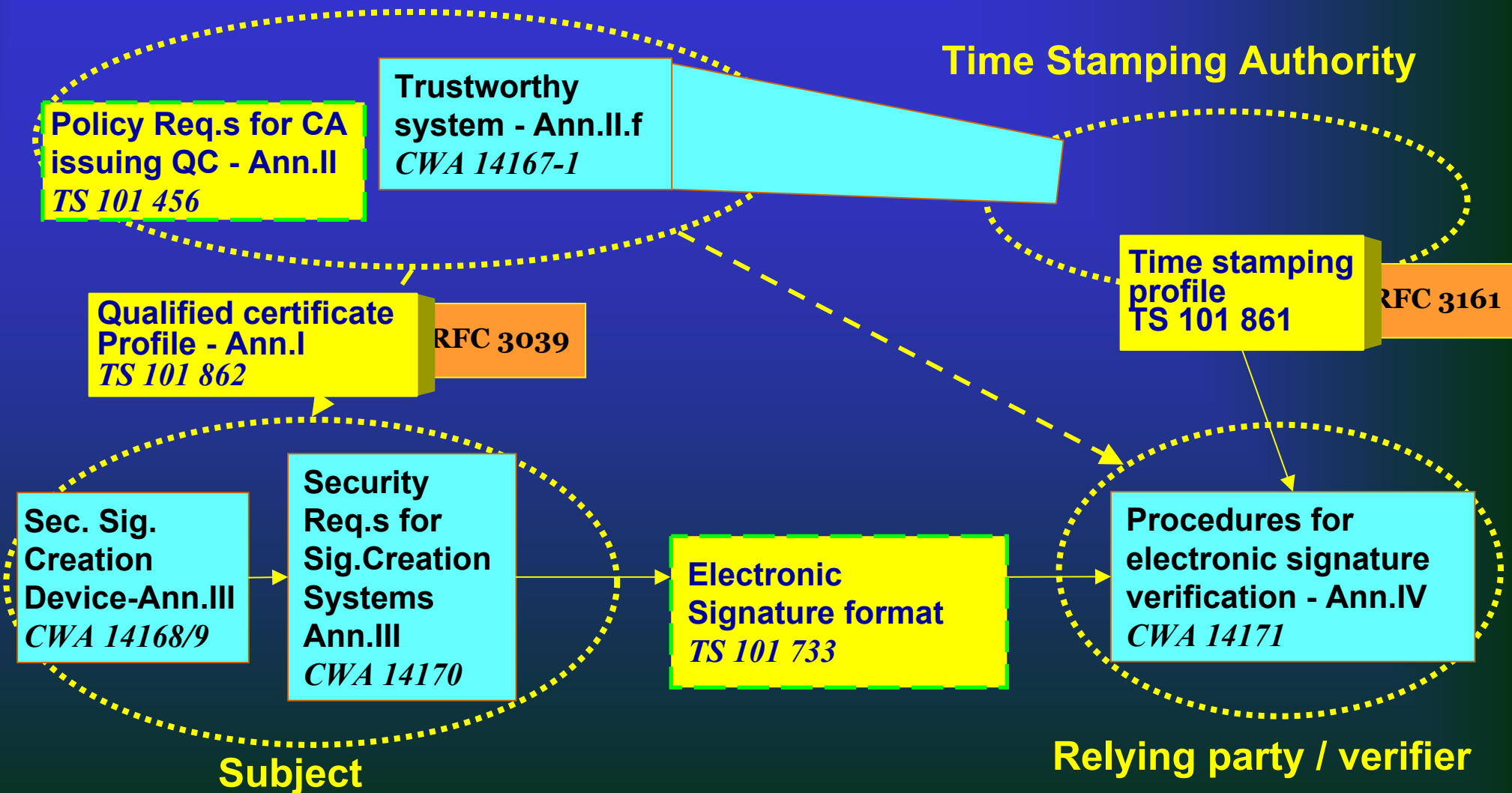


EESSI Phase 2 Roadmap

CEN/ISSS E-SIGN

ETSI ESI

Certification Service Provider

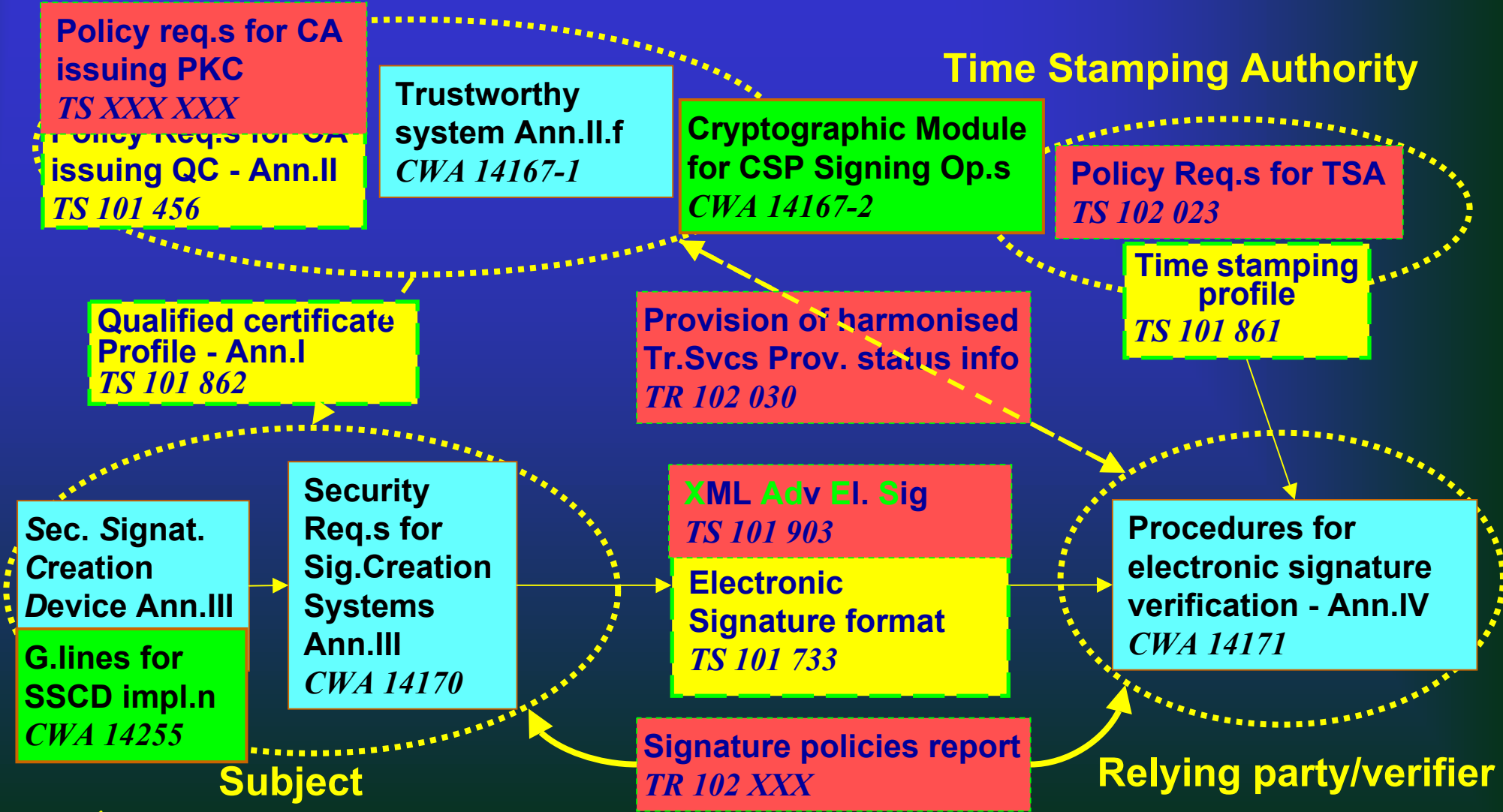


EISSI Phase 3 Roadmap

CEN/ISSS E-SIGN	ETSI ESI
CEN/ISSS E-SIGN	ETSI ESI

Certification Service Provider

Time Stamping Authority



Signature Policy

Insieme di norme, che regolamentano la creazione e la verifica delle firme elettroniche, nel rispetto delle quali una firma elettronica può essere considerata valida in un particolare contesto transattivo.

*Codici degli standard di fase 2 e 3 - CEN/ISSS Workshop
Electronic Signatures (CEN/ISSS WS/E-Sign).*

- **CEN Workshop Agreements (CWA)**
 - CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
 - CWA 14167-2: Cryptographic Module for CSP Signing Operations — Protection Profile (*Phase 3*)
 - CWA 14168: Secure Signature-Creation Devices, version 'EAL 4'
 - CWA 14169: Secure Signature-Creation Devices, version 'EAL 4+'
 - CWA 14170: Security Requirements for Signature Creation Systems
 - CWA 14171: Procedures for Electronic Signature Verification
 - CWA 14172: EESSI Conformity Assessment Guidance
 - CWA 14255: Guidelines for the implementation of SSCD (*Phase 3*)

- Technical Specifications (TS) e Technical reports (TR)
 - TS 101 456 – Policy requirements for certification authorities issuing qualified certificates
 - TS 101 733 – ES Formats → RFC 3125 e 3126
 - TS 101 861 – Time stamping profile
 - TS 101 862 – Qualified Certificates profile
 - TS XXX XXX – Policy req.s for CA issuing PKC
 - TS 102 023 – Policy Requirements for TSA
 - TS 101 902 – XML Advanced El. Signature
 - TR 102 038 – Signature policies report
 - TR 102 030 – Provision of harmonised Trusted Services Provider status info

Codice in verde:
approvato

Codice in rosso:
work in progress

Sviluppi futuri = 2002

- Estensione di SSCD ad art. 5.2

CEN/ISSS
(non ancora
finanziato)

- Requirement per Smart Card usate come SSCD

- Estendere l'ambito di applicabilità delle Signature policy: firme multiple, controfirmatura, ecc.

- Definire i requisiti per la certificazione di ruoli e attributi

ETSI

- Armonizzare, quanto fatto, con gli altri body di standardizzazione internazionali

*Finanziato
(da Commissione)*

- ...e poi: definire, in accordo con i vari paesi membri della CE, modalità e protocollo di comunicazione dello stato di un Trusted Services Provider al momento in cui:

- è stato rilasciato un certificato / time stamp ad un titolare,
- è stato firmato / time stamped un documento,
- viene verificato un documento firmato.

ETSI
(non ancora
finanziato)

Ma, in definitiva, si utilizzeranno?

Si vedrà.

Fattori positivi

Da un lato:

**ampia partecipazione di industria, P.A.,
organi di valutazione, da quasi tutti i
paesi europei → “coregulation”**

Dall'altro:

il parere del Commissario Europeo

Liikanen

Estratto di un suo discorso del 19/6/2001

- The purpose of EESSI is to ensure that the ***legal requirements*** (for a better legal recognition of electronic signatures in the EU) ***are implemented by workable, interoperable solutions.***
- ... standards in support of the e-signatures Directive must:
 - be open
 - be internationally agreed
 - be sufficiently flexible to cover different business models
 - provide secure solutions for electronic signatures.

These basic criteria are met by EESSI.

Therefore, the EESSI deliverables are a ***candidate*** to become "***reference standards***" for the implementation of the e-signatures Directive.

- ...

Estratto di un suo discorso del 19/6/2001 (2)

- For this reason it would be important that ***EESSI deliverables are as widely disseminated and promoted as possible.***
- Standards don't promote interoperability per se. Only standards that are widely used have an impact on the market.
- I appreciate that ***EESSI has found the right balance.***
- ...

Conclusione di Lükanen:

I consider EESSI as a success story.

“ “ “ *e comunque* “ “ “

La Commissione ha attivato un gruppo di 6
“independent experts” con il compito di
verificare la rispondenza dei “prodotti” EESSI
alle esigenze della Direttiva 1999/93/EC.

La fine dei lavori entro
Marzo 2002

Grazie per
l'attenzione

F I R D I G