IDABC
Pan-European
eGovernment Services

Results of the IDABC Bridge / Gateway Certification Authority pilot project

Gzim Ocakoglu
European Commission
Enterprise and Industry Directorate General

ITAPA Congress
Bratislava, 22 November 2005

Outline

- Introduction to IDABC Programme
- Security measures within IDABC
- Bridge/Gateway CA Project Results
  - Project History
  - Bridge/Gateway CA Pilot
- Next steps
- Conclusions

IDABC Programme

http://europa.eu.int/idabc

Objectives	Identifying, supporting and promoting the development and establishment of **eGovernment services**
Target groups	Administrations, Business and Citizens
History	Experience since 1995, IDABC is a follow-up to IDA and IDA II Programmes
Duration	5 years (2005-2009)
Global budget	**148.7 million EUR**
	Actions are Commission-driven and implemented via public procurement
Managed by	Enterprise and Industry Directorate General (idabc@cec.eu.int)

IDABC Programme

http://europa.eu.int/idabc

Key elements of IDABC Work Programme 2005:

- **Your Europe Portal** (http://europa.eu.int/youreurope)
- More than **20 sectoral projects in policy areas of EU** managed by other DGs, e.g. **PLOTEUS, LISFLOOD, SANREF, TRACES**
- More than **20 projects** designed to **support sectoral projects** and **eGovernment services generally** by providing basic infrastructure (**S-TESTA, eLINK, CIRCABC**), security measures (**eID**), interoperability measures (**European Interoperability Framework, XML Clearing house**), spread of good practise (**OSS repository, eGov observatory**)

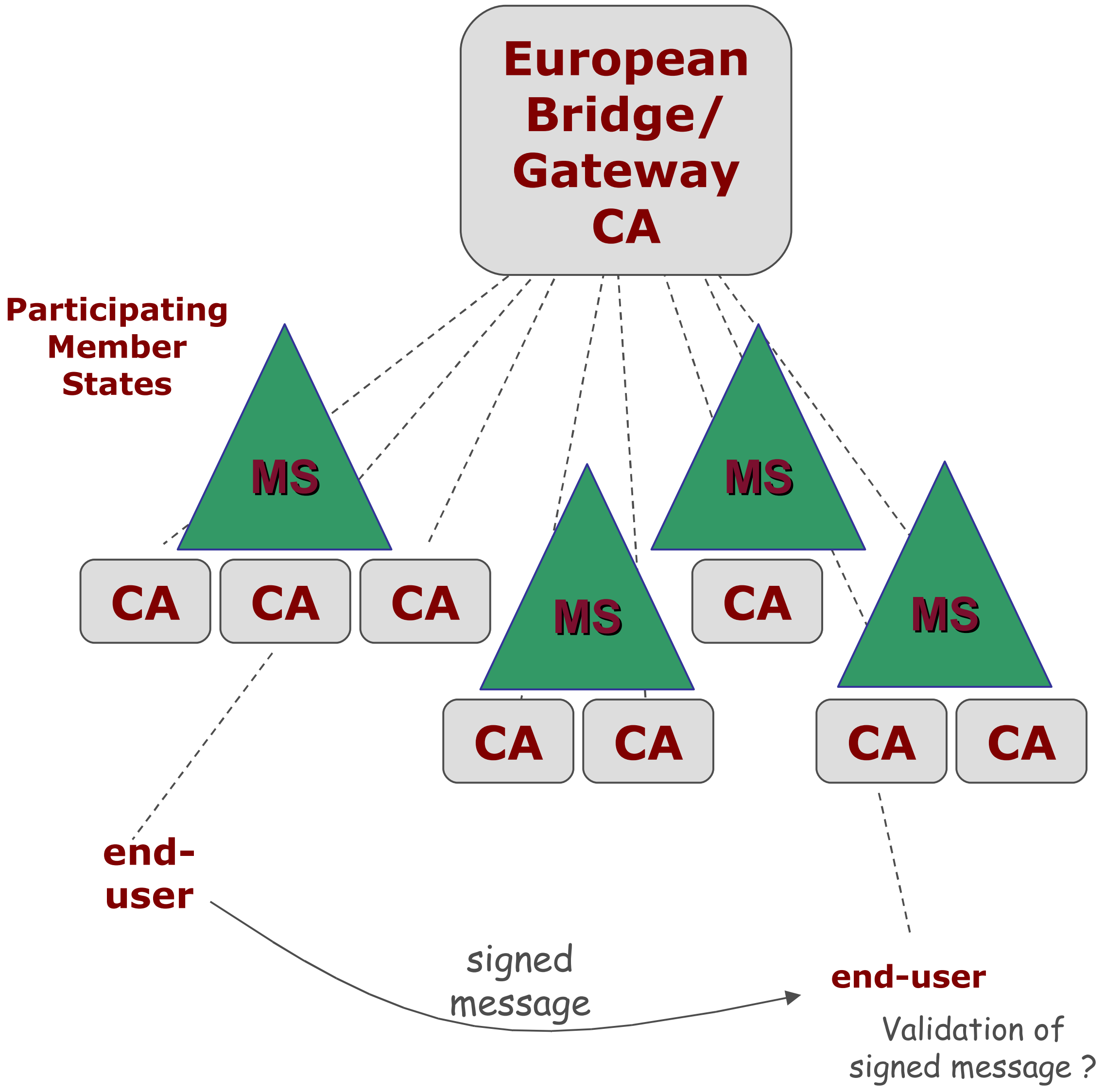
IDABC Security Measures (1)

- Security instruments (consultancy)
  - Update IDA self-assessment security questionnaire
  - Risk analysis and security assessments (audits) of PEGS and PCI’s
- Common Identity Management Service (CIMS) – project managed by DG DIGIT
- Certification Services
  - Delivery of server and user certificates (PKI)
  - Dedicated services e.g. time-stamping

IDABC Security Measures (2)

- Preliminary study on mutual recognition of eSignatures
  - Survey on eGov applications (e.g. eProcurement) requiring eSignatures
  - Assessment of legal and technical issues
  - Proposal for a mutual information mechanism on legal requirements for eSignatures
- eIdentity interoperability for PEGS
  - Survey of existing eID national schemes (technical and legal implementations)
  - Market assessment of IDM solutions
  - Proposal for eID interoperability solution for the PEGS

Bridge/Gateway CA Model



Validation of signed message ?

BGCA Project History

- 1999 : First PKI CUG’s established under the IDA Programme : issue of interoperability (recognition) of national digital certificates was raised by MS (Member States)
- July 2002 : Bridge CA Feasibility Study issued as a result of MS request
- July 2003 : “WP1” : Analysis of Bridge CA Requirements completed and reviewed
- July 2004 : Selection of ETSI TSL standard as technical solution for BGCA Pilot
- December 2004 : BGCA Pilot Launch

Defining the IDA BGCA Model

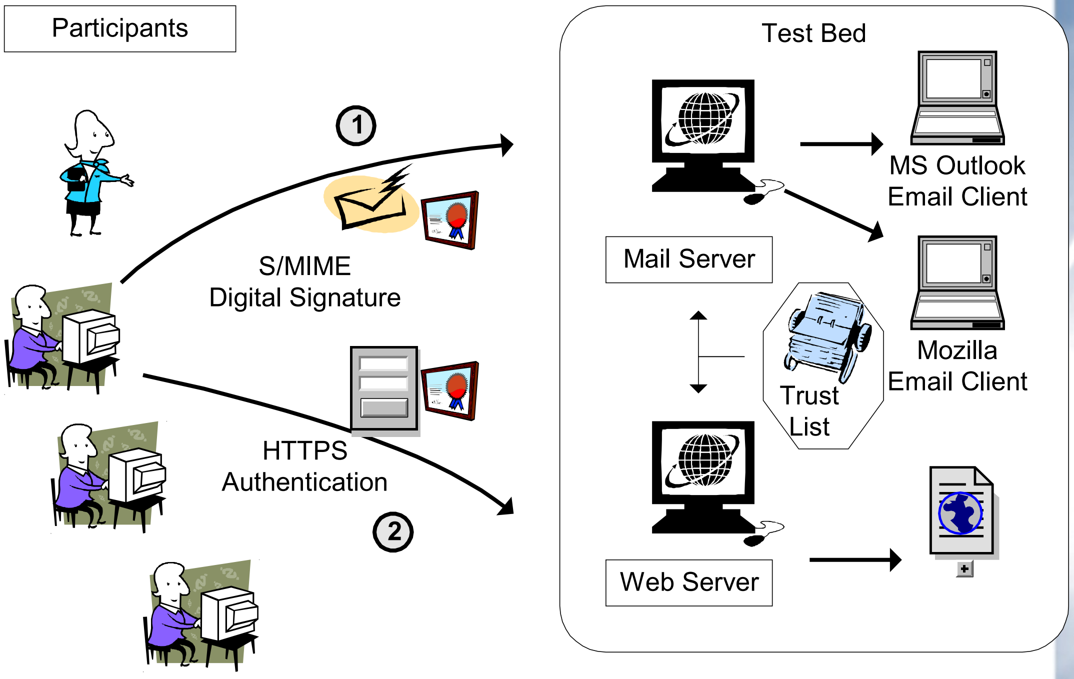
- Reference documents : http://europa.eu.int/idabc/en/document/3235/5585
- Trust list usage recommendations
  - Usage of Trust lists : solely for distribution purposes
  - 3 trust functions will be explored (add, remove or accept CA's from trusted lists)
  - Standard : use of ETSI TS 102 231 with modified profile
  - Applications : SSL mutual authentication and S/MIME
- Network Architecture
- Test Programme

BGCA Pilot Project

- Part 1 : Pilot
  - Set-up of BGCA Infrastructure
  - Running of Pilot Tests
  - Report on test results
  - Report on technical requirements for MS administrations
- Part 2 : Recommendations for operational Bridge/Gateway CA
  - Certificate Practices Statement for operational BGCA
  - Participation documents (including procedures) for operational BGCA
  - Recommendations for extension of Pilot to Industry
  - Recommendations for end-users

Part 1: BGCA Pilot

- 9 participating countries
  - Belgium
  - Italy
  - Germany
  - Finland
  - Czech Republic
  - Estonia
  - Slovakia
  - Slovenia
  - Iceland



Functionality Tests

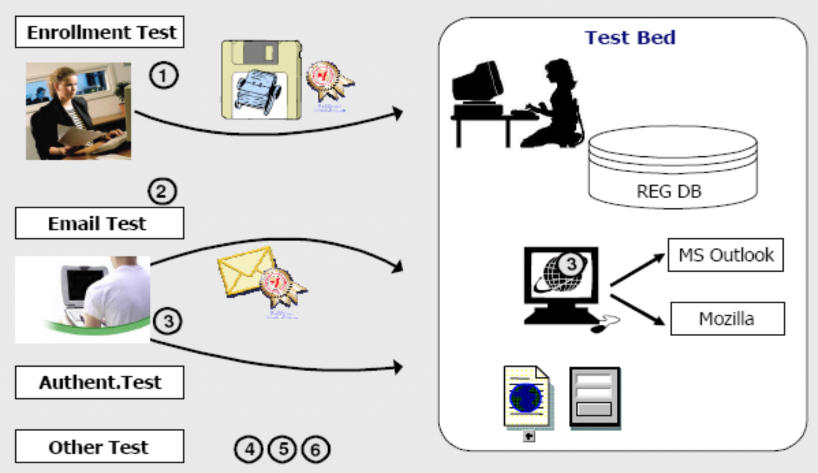
- Testing basic Trust List functions and Bridge and Gateway CA actions:
  - Issue a Trust List
  - List the contents of a Trust List
  - Add a CA Certificate to the Trust List
  - Remove a CA Certificate from the Trust List
  - Validate the signature of the Trust List

Interoperability Tests

- Test following actions of the Participant CA :
  - Join the Bridge and Gateway CA Pilot
  - Import the “Trust List” into an application (Outlook, Mozilla)
  - Communicate via S/MIME message to the test bed
  - Log on to Test Bed web site using certificate
  - Re-Sign and publish the Trust List

Cross MS Test

- Similar tests as the interoperability test, but here between MS
- Cross MS test between Estonia and Slovenia performed with success
  - signed e-mail between end-users:
    - *Signer certificate checked for trust path + issuer certificate content;*
    - *existing certificate used for reply;*
    - *signature has been verified (OK)*



BGCA Pilot : Interoperability test conclusions

- ☺ Principle of working with Trust List (TSL) : OK.

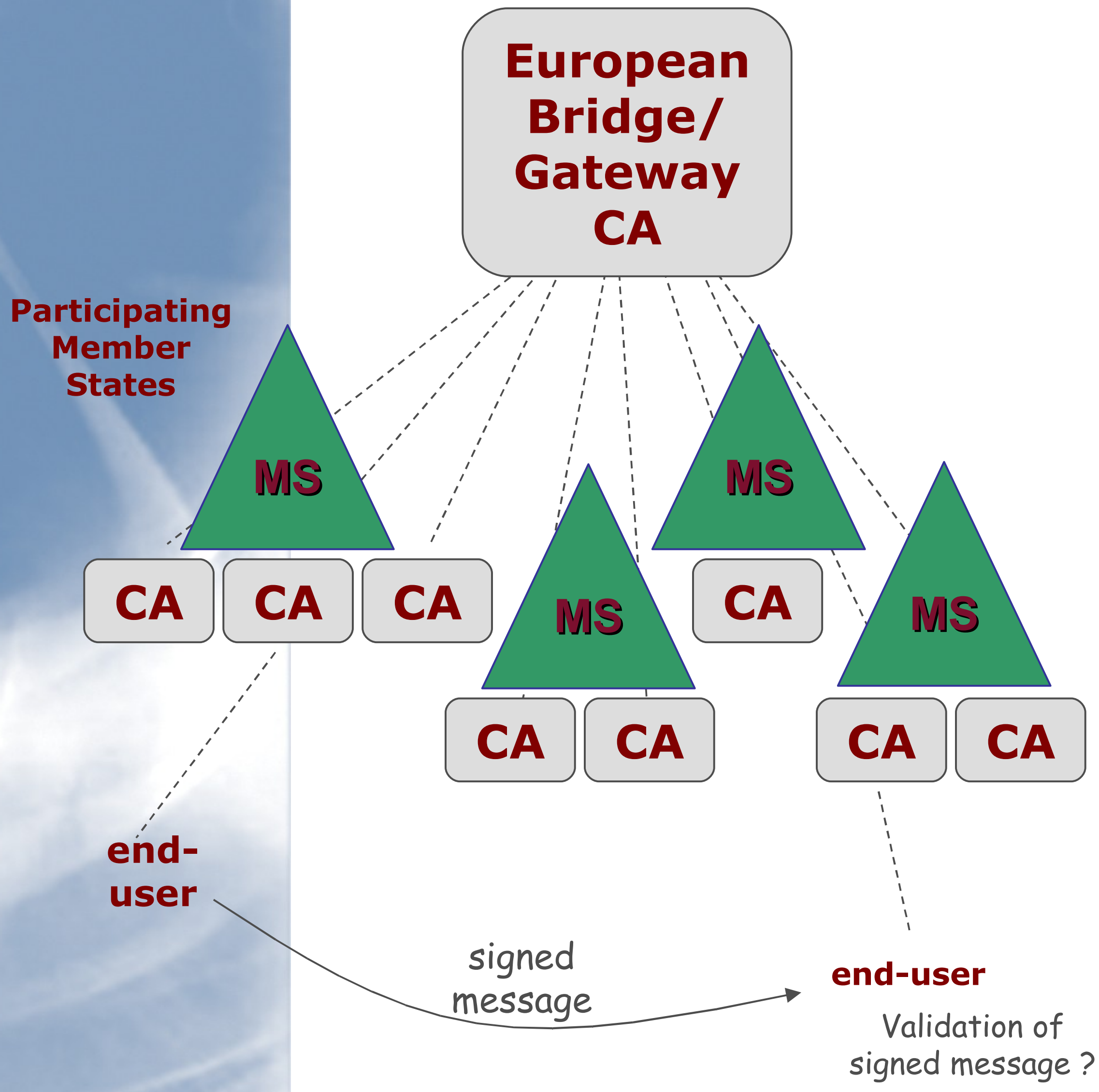
- ☹ No e-mail client nor SSL-browser is actually yet supporting TSL ➔ manual intervention to set-up a working system !

  - ☹ Experience with the different e-mail clients: Problems have been encountered with Lotus Notes. Contractor notified IBM
  - ☺ IBM acknowledges that version 7.0 resolves the issue.

- ☺ Distinction was correctly made between a test with *real CAs* (CAs under trusted TSL) versus *fictious CAs* (i.e. non-trusted CAs). It could be clearly deducted whether an e-mail was trustworthy or not.

- ☺ Cross MS test between Estonia and Slovenia performed with success (signed e-mail: Signer certificate checked for trust path + issuer certificate content; *Used existing certificate for reply; received e-mail and signature verified has been verified OK.)*

Part 2 : Recommendations for operational Bridge/Gateway CA


European Bridge/ Gateway CA
Participating Member States
MS
MS
MS
MS
CA
CA
CA
CA
CA
CA
CA
CA
end-user
signed message
end-user
Validation of signed message ?

Bridge Practices Statements
(CPS + signature policy)
in issuing TSL to Participating Member States CAs

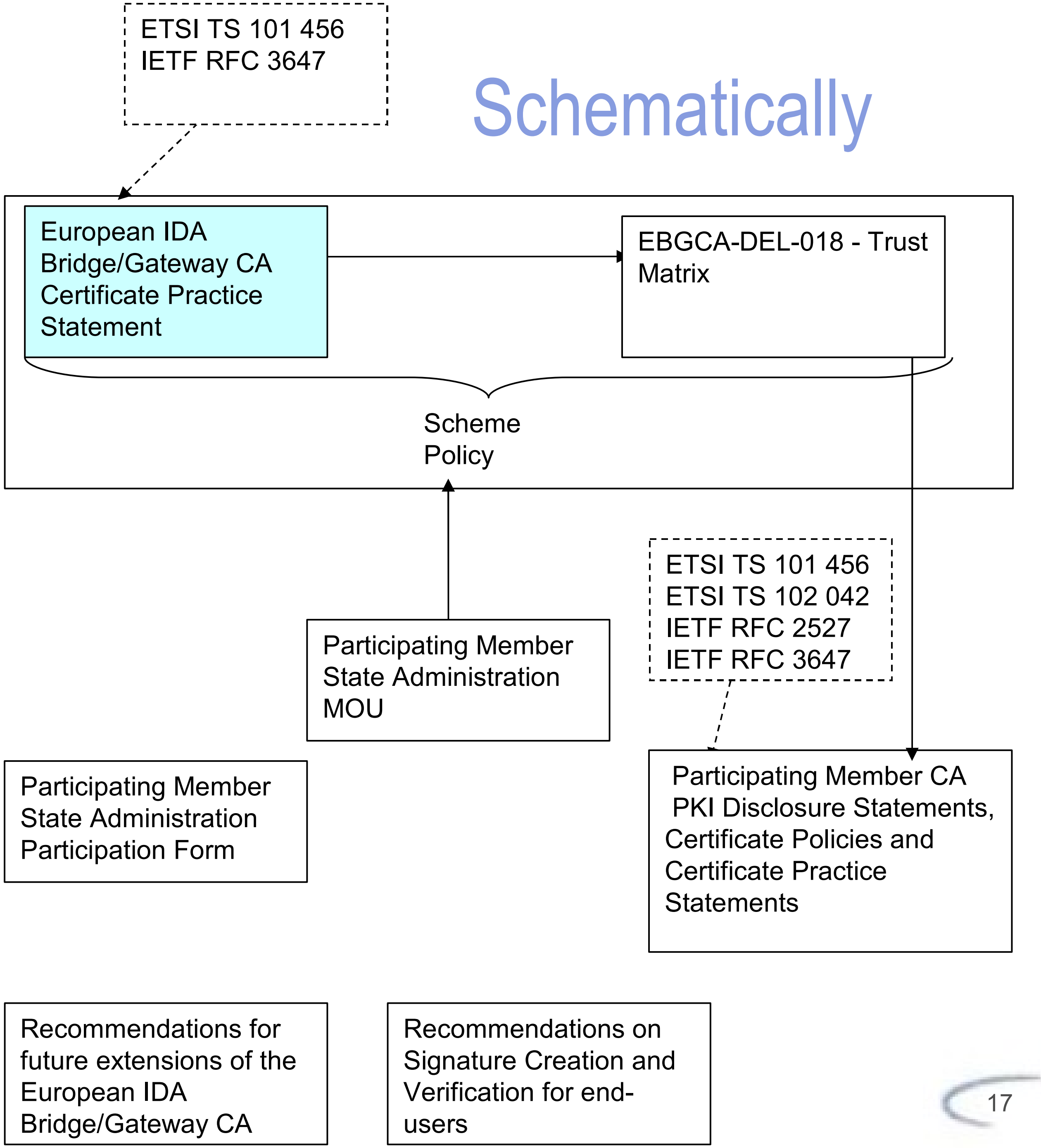
MOU agreement

PKI Disclosure Statement
including “Trust Validation Info” in each Certificate Policies for each Participating CA

Trust Equivalence Matrix
between Certificates types accross Participating CAs

Signature Validation Guidelines
in assessing trust in end-user signature

Schematically



ETSI TS 101 456
IETF RFC 3647

European IDA Bridge/Gateway CA Certificate Practice Statement

EBGCA-DEL-018 - Trust Matrix

Scheme Policy

Participating Member State Administration MOU

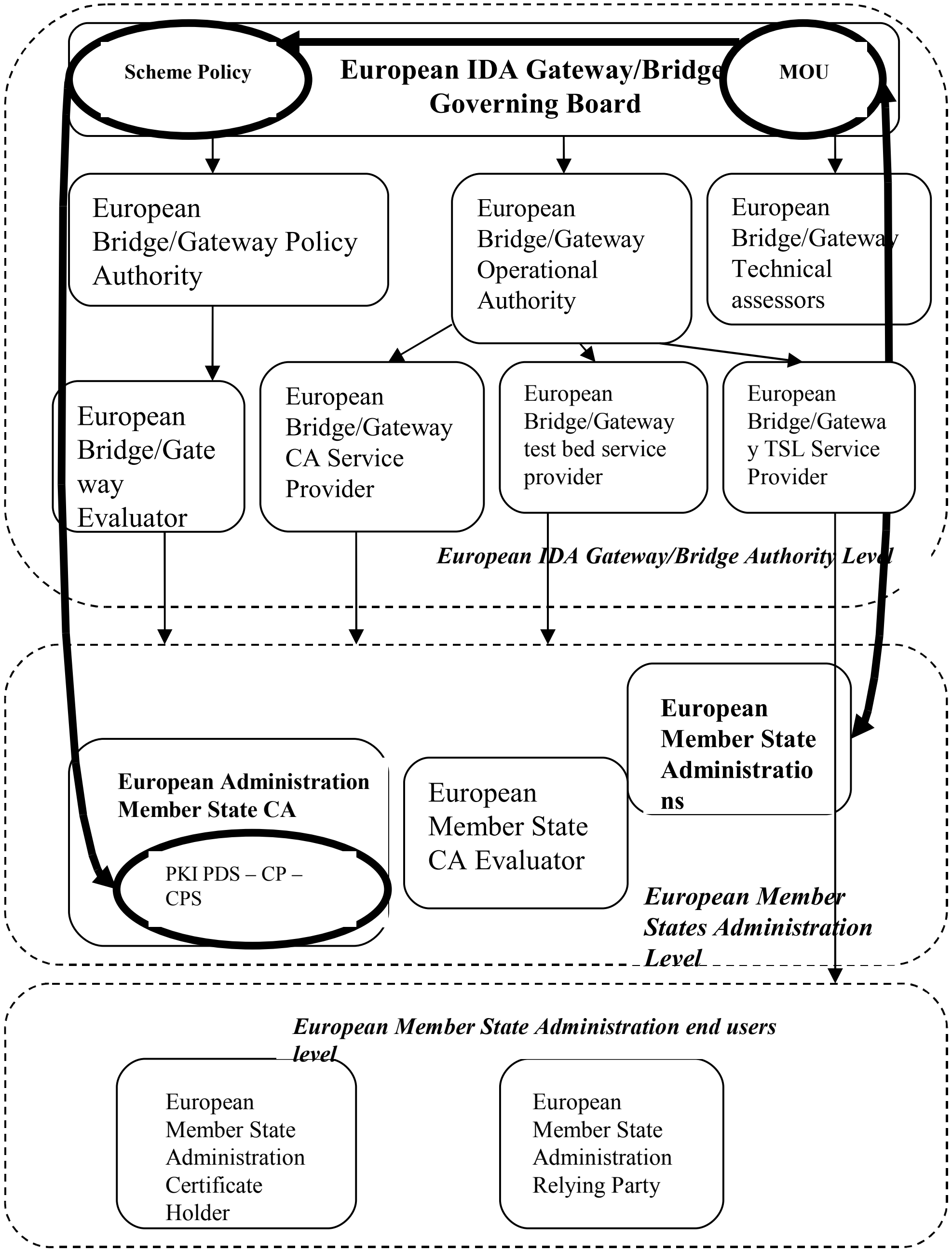
ETSI TS 101 456
ETSI TS 102 042
IETF RFC 2527
IETF RFC 3647

Participating Member State Administration Participation Form

Participating Member CA PKI Disclosure Statements, Certificate Policies and Certificate Practice Statements

Recommendations for future extensions of the European IDA Bridge/Gateway CA

Recommendations on Signature Creation and Verification for end-users



Scheme Policy

European IDA Gateway/Bridge Governing Board

MOU

European Bridge/Gateway Policy Authority

European Bridge/Gateway Operational Authority

European Bridge/Gateway Technical assessors

European Bridge/Gateway Evaluator

European Bridge/Gateway CA Service Provider

European Bridge/Gateway test bed service provider

European Bridge/Gateway TSL Service Provider

European IDA Gateway/Bridge Authority Level

European Member State Administrations

European Administration Member State CA

PKI PDS – CP – CPS

European Member State CA Evaluator

European Member States Administration Level

European Member State Administration end users level

European Member State Administration Certificate Holder

European Member State Administration Relying Party

Recommendations - Extension towards business and citizens

- Businesses and Citizens
  - Liabilities framework:
    - Contractual relationships to be established
    - TSL Provider should as a minimum be liable for damage caused to any entity or legal or natural person who reasonably relies on that TSL
  - Independent, neutral European Body : overall responsible for the European IDA Bridge/Gateway Authority
    - role and responsibilities of the EBG Governing Board towards Member States, the Administration supervising the national CA application, national Administrations, businesses and citizens
  - Additional contractual arrangements must be drawn between the European IDA Bridge/Gateway Governing Board and its contractors
  - Governing Board must be composed of independent and highly trusted persons, not all members of the EBGCA and be apart from the operational organisation of the EBGCA

Next steps for an operational BGCA

- Definition of ownership of BGCA and deployment
  - Setup of legal advisory board within EU
    - Legal opinion on the applicability of the European Directive 1999/93/EC on the EBGCA activities
    - Choice of legal instrument (MOU), agreement on Governing Body, Liability, applicable law, supervision scheme, concept of PDS and Trust Matrix, …
  - Setup of Governing Board
- To obtain TSL-support in email clients +browser ➔ necessary pressure @ vendors
- Some technical :
    - Central validation services
    - Central Time-stamping

Conclusions

- Bridge/Gateway CA Pilot was set up and worked properly from technical viewpoint
  - Concept of TSL is fine
  - Application software vendors need to include TSL in their product !
- Recommendations for an operational European Bridge/Gateway CA were made
  - Prerequisites :
    - Agreement on BGCA Governing Body, MoU format and concept of PDS and Trust Matrix
    - Definition of ownership of BGCA and deployment
  - Strong political commitment is required (need of EU driven actions)

More Information :

Web: http://www.europa.eu.int/idabc

E-mail: idabc@cec.eu.int

Address:
IDABC Secretariat
DG Enterprise & Industry
IDABC – BREY 11/248
European Commission
B-1049 Brussels, Belgium

THANK YOU !