The IDABC Bridge / Gateway Certification Authority: a model of “eID interoperability”

Gzim Ocakoglu
European Commission
DG DIGIT/01(IDABC)

IDABC eID Interoperability Workshop
Brussels, 10 May 2007
Outline

• Bridge/Gateway CA Model
  – BGCA History
  – Bridge/Gateway CA Pilot
  – conclusions

• Assessment
Problem statement: why a Bridge/Gateway CA?

- IDA PKI deployed as a stop-gap solution in IDA II Programme
  - Members of sectoral networks should rely on national PKIs
    (Currently not available for most civil servants)
- eEurope Action Plan
  - support for electronic signatures in public administration
- Member States’ policy
  - ability to use the electronic certificates issued by their national CAs in pan-European business
- IDA II programme policy
  - encourage interoperability, use of standards, use of e-signature, etc.
  - Conclusions from previous projects
Scope of the Bridge/Gateway CA

- to establish an intermediate trust infrastructure to allow a MS or the Commission to have trust and confidence in electronic certificates issued at the national level to civil servants participating in IDABC networks.
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
• July 2002 : Bridge CA Feasibility Study issued as a result of TAC 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
• November 2004 : “WP1.2” deliverables available
• December 2004 : BGCA Pilot Launch
• December 2005 : Presentation of Pilot Results
Summary of Bridge CA Feasibility Study


- Need of strong political support (e.g. explicit commitment from the European Commission)
- Need of governing body with high level participation of MS in the body
- Architecture: Modified Bridge CA or BGCA (distribution of signed trust lists)
- Need of some form of harmonisation of certification policies
- Need of agreed minimum standards and operating procedures for CA’s
- Operation of the Bridge: suitable European agency or external contractor?
- Need for a pilot
Validation of signed message?
Defining the IDA BGCA Model


- 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

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

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

L  Experience with the different e-mail clients: Problems have been encountered with Lotus Notes. Contractor notified IBM

J  IBM acknowledges that version 7.0 resolves the issue.

J  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.

J  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

- MOU agreement
- PKI Disclosure Statement including “Trust Validation Info” in each Certificate Policies for each Participating CA
- Trust Equivalence Matrix between Certificates types across Participating CAs
- Bridge Practices Statements (CPS + signature policy) in issuing TSL to Participating Member States CAs
- Signature Validation Guidelines in assessing trust in end-user signature

Participating Member States

- end-user
- signed message
- Validation of signed message?
European IDA Bridge/Gateway CA Certificate Practice Statement

Scheme Policy

ETSI TS 101 456
IETF RFC 3647

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

ETSI TS 101 456
IETF RFC 3647

EBGCA-DEL-018 - Trust Matrix

Participating Member State Administration MOU


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

Recommendations on Signature Creation and Verification for end-users
EBGCA stakeholders

• **EBGCA Authority Level**
  – BGCA Governing Board or Body: with representatives of all concerned parties
    • E.g. European Commission or agency
    • MS representatives, responsible for the national PKI’s
  – BGCA Policy Authority: implementation of the BGCA Policy scheme (including CP’s mapping)
  – BGCA Evaluators: independent agents that will determine trust level of requesting CA’s
  – BGAC Operational Authority: coordination of operation of the BGCA (CA and RA services, TSL services, tesbed services)

• **European MS Administration level**
  – MS administration
  – MS evaluator (e.g. existing national supervision of accreditation body)
  – MS CA service provider

• **European MS Administration end-user level**
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 È 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)
Assessment

• BGCA is a practical interoperability model for PKI based eIDM systems
• An implementation of the BGCA could constitute part of the solution (for PKI-based systems)
• What are the issues :
  – Technical scalability?
  – Add a validation model as well
  – Need for organisational and legal agreements (like in any solution!)
Thank you!

More Information:

Web: http://www.ec.europa.eu/idabc
E-mail: idabc@ec.europa.eu
Address: IDABC Secretariat
         DG DIGIT/01
         IDABC – MO34 03/88
         European Commission
         B-1049 Brussels, Belgium

Thank you!