Interoperable digital certificates for e-commerce

Dr Andreas Mitrakas
GlobalSign

The Open Group Conference, Helsingor, 27 April 1999
Context

Basic “key” elements of our trade culture

★ Identifiers
★ Proofs
★ The need for Privacy
Context

Basic “key” elements of our trade culture

- Identifiers: Digital IDs
- Proofs: Digital Signatures
- The need for Privacy: Encryption
Market Volume

Source Datamonitor: Market Volume PKI (certificates)
Market Volumes

☆ Datamonitor: Market Volume PKI: 2001, $m1800, 1/3 Europe, growth rate Europe > US

☆ Forrester Research: “The average corporation currently spends more on coffee and soft drinks than on network security; we expect this to change”

☆ John Maynard Keynes: “I would rather be vaguely right than precisely wrong”
Market Volumes

★ Aligned growth rate with e-commerce

- number of Internet Users: 97 million in 1998, 320 million in 2002
- e-commerce market volume: $32 billion in 1998, $426 billion
Agenda

★ Introduction
★ Certification Authorities
★ A profile of GlobalSign
★ Interoperability
★ A Legal Framework
★ Conclusions
Certification Authorities

★ Trusted Third entity that issues, publishes and revokes certificates
  • market recognition: partners, brand-name
  • licensing from the government

★ Certificate classes
  • May issue different “classes” of certificates depending on the level of ‘trust’
  • Banking vs Online Publishing
  • verification: is that person the person who he/she claims to be?
“Leading European Trusted Third Party based on an International Network of Certification and Registration Authorities which all meet the same accreditation requirements, follow the same verification procedures and co-brand their certificates in order to achieve international recognition of digital certificates and world-wide interoperability of CAs and RAs”.
GlobalSign

GlobalSign:

a network of local Certification and Registration Authorities

combining national trust credentials by local presence and international recognition and interoperability by uniform rules

combining a minimum common framework based on EC directives and local legislation

diverse legal regulations in the European Union can be better addressed through a network of RAs.
A Clearing Network

Int Credit Card Comp

Clearing House

Bank

Bank

Clearing House

Bank

...

A Certification Network
GlobalSign’s European CA/RA Network

- Italy
- Belgium
- Luxembourg
- Austria
- Netherlands
- UK
- Greece

- EC projects: 11 member States
GlobalSign: 120,000 certificates issued in 1998

- Belgium: 6%
- Germany: 7%
- UK: 8%
- Italy: 5%
- Netherlands: 5%
- France: 5%
- Japan: 5%
- United States: 5%
Agenda

- Introduction
- Certification Authorities
- A profile of GlobalSign
- Interoperability
- A Legal Framework
- Conclusions
Issues of interoperability

★ Legal diversity

★ PKI industry faces a balkanised legal environment

★ Less obvious problems in the technical front

★ CA instruments: CAs compelled to co-ordinate their practices with the Law through their CPS and Certification Policies
GlobalSign’s CPS

★ GlobalSign publishes its Certification Practice Statement describing in great detail the practices and procedures it uses for the issuing and management of certificates.

★ The CPS of GlobalSign is subject to annual auditing by a recognized auditor. Suggestions have been appropriately incorporated in the current version.
A recognized CPS

- GlobalSign’s CPS is compatible with most legal obligations imposed by laws in EU member states and the EU draft directive and the draft laws of the Belgium and the Netherlands.
- GlobalSign acknowledges its responsibility as a CA through a comprehensive insurance programme.
- As a European CA GlobalSign offers full protection to consumers according to the EU directives on consumer protection and privacy.
GlobalSign follows the PKIX WG recommendations, e.g., the RFC 2459 draft.

GlobalSign’s Top root and primary roots follow the PKIX recommendation.

To serve users of Netscape, GS adds non-critical Netscape proprietary extensions to clients and the lowest level of GlobalSign’s signing roots.

Next generation of certificates will not require the proprietary extensions of browsers any more.
GlobalSign certificates have been tested on software packages:

- Netscape browser and server
- Microsoft browser and server
- Opera browser
- Apache server

and on operating systems

- Win NT4, ’98, 3.1
- Linux

GlobalSign certificates can be used on many more packages and OSs depending on user needs and requests.
Technical Interoperability III

- Although GlobalSign currently does not have full scale procedures for interoperability tests it is currently on the way of implementing interoperable standards with other CAs.

- Discussion and exchange of opinion through mailing lists
Agenda

★ Introduction
★ Certification Authorities
★ A profile of GlobalSign
★ Interoperability
★ A Legal Framework
★ Conclusions
Towards Security Interoperability

- **Self-regulation**

- As market grows it will be increasingly necessary to address the issues of interoperability through discussion in appropriate industry fora.

- Self-regulation essential for interoperability to set a standard of PKI services, technical requirements, organizational matters and additional security measures.
Towards Security Interoperability II

★ Positive Law

★ A homogeneous legal approach on interoperability will reduce transaction costs and increase the level of trust in providing CA services

★ Uniformity is critical in areas like consumer transactions and professional usage
A self-regulation based framework

★ The ICC ETERMS Repository

★ The ICC ETERMS Repository can be used to register, publicize and access a CPS

★ The ICC ETERMS Best Practice Rules can provide an appropriate forum for the discussion and conclusion of a uniform way to address interoperability issues

★ Adherence to the ICC ETERMS BPRs can be used within a benchmarking system to assess compliance with interoperability standards
Where do we go from here?

As e-comm progresses...

Business Credentials

Identifiers

Payment Security

Legal Security Tax Logistics

Digital Signatures Encryption Digital IDs

Business Auditors Certification Authorities Clearing House
Tentative Conclusion
Tentative Conclusion

- Widely applied information security consistent legislation to support interoperability of CA certs
- Self-regulation to dynamically pursue an industry supported solution for interoperability
- The ICC ETERMS can play a role in an increasingly complex information security environment based on PKI