ABA PKI Evaluation Guidelines: The Law and Digital Signatures

Information Security Committee
American Bar Association (ABA)
Section of Science and Technology

Presentation to The Open Group Conference
Copenhagen, Denmark
27 April 1999
Introduction

✔ Information Security Committee, Section of Science and Technology, Electronic Commerce Division

✔ Over 300 Technologists and Lawyers from more than 15 countries

✔ Digital Signature Guidelines, 1996 (see http://www.abanet.org/scitech/ec/isc/dsgfree.html)
Introduction (cont’d)

✓ Michael Baum - VeriSign (U.S.)
✓ Joe Alhadeff - Oracle (U.S.)
✓ Janjaap Bos - DSEMCO B.V. (Netherlands)
✓ Emily Frye - VeriCorp (U.S.)
✓ Bill Kennair - CyberNotary Association UK (U.K.)
✓ Charlie Merrill - McCarter & English (U.S.)
✓ Randy V. Sabett - SPYRUS, Inc. (U.S.)
✓ J. F. Sauriol - Labcal Technologies (Canada)
Goals today

✓ Introduce PKI Evaluation Guidelines (PEG)
✓ Interactive dialog regarding diverse requirements and initiatives
✓ Collaboration/harmonization/assimilation
✓ Discuss need for recognized global standard
✓ Formalized baseline for global interoperability of PKI
Challenges in PKI

✔ Trust, confidence, certainty
✔ Risk management
✔ Interoperation
✔ Self-regulation
✔ Quality assurance
PKI Evaluation Guidelines (PEG)

- Project begun in late 1996
- Extends beyond digital signatures to support diverse applications and entities in a PKI
- Intended to bridge legal, business, and technical aspects
- Guidelines, not criteria
- Work-in-progress
The PEG Audience

Anyone involved in PKI deployment, including:

- Criteria (policy) adopting or defining bodies
- Accrediting body
- Evaluators
- Authors of CPs
- Adopters of CPs
- Those involved in dispute resolution
PEG Terminology

✓ “Accreditation” of evaluators of PKI
✓ “Evaluation”: broad term, encompassing
  – “Assessment” of PKI for purposes of building legal and technical interoperability
  – “Auditing” of PKI components after deployment to determine whether the PKI conforms to the applicable CP
One example of process…
PEG Structure

Main topics:

- Understanding PKI
- Process for PKI Evaluation/Accreditation
- Elements of PKI Evaluation/Accreditation
- Legal Preface
- PEG Methodology for Evaluation/Accreditation
- PKI Evaluation Guidelines
- Appendices
PEG Structure (cont’d)

✅ Address diverse PKI models
  - “One size does not fit all”

✅ Matrix concept
  - RFC2527 (also known as PKIX Part 4) provides the rows
  - Different vertical markets comprise the columns (e.g. the financial services industry)
PEG Structure (cont’d)

✓ Introduction
✓ General Provisions Covering Legal/Business Issues
✓ Initial Validation of Identity and Authority
✓ Certificate Life Cycle Operational Requirements
✓ CA Facility and Management Controls
✓ Technical Security Controls
✓ Certificate and CRL Profiles
✓ Specification Administration
✓ Some differences from RFC 2527
Selected Legal and Policy Issues

✓ Legal regimes
✓ Consumer and privacy issues
✓ Distinction between CP and CPS
✓ Liability of parties in PKI
Selected Legal and Policy Issues (cont’d)

✓ Legal presumptions
✓ Evidentiary issues
✓ Separation of roles in certificate lifecycle
✓ Incorporation by reference
Current state of international law

✔ UNCITRAL
  – Model Law on Electronic Commerce
  – *Electronic Signature Rules*

✔ OECD: Cryptography Guidelines

✔ ICC: GUIDEC

✔ European Union
  – *Directives on Electronic Signatures*
  – *Directives on Electronic Commerce*

✔ UINL: *Ongoing educational process*
Civil law and common law

✓ Codification versus precedent through litigation

✓ Possible differences
  – Binding nature of judicial decisions
  – Legal Presumptions
  – Incorporation by reference
  – Form requirements

✓ Base all future actions on legislation in either type of jurisdiction or leave it to the open market?
Consumer and privacy issues

✓ Does the concept of “consumer” map to specific parties in a PKI?

✓ Need for minimum requirements between parties?
  – obligation to protect private key
  – obligation to verify certificate status
  – liability allocation
  – notice and disclosure

✓ Collection & use of personal information

✓ Applicability of various guidelines & initiatives
Distinction between CP and CPS

✅ CP specifies the requirements (the “what’s”)

✅ CPS specifies how the CA complies with those requirements
  – the “how’s”

✅ Which governs rights between the parties when difference between the CP and CPS?

✅ Model independent...
Separation of roles in the certificate lifecycle

LEGEND
CA = Certification Authority
CMA = Certificate Management Authority
RA = Registration Authority

Users (subscribers and/or relying parties)
 Liability of parties in PKI

✓ CA liability to relying party for wrongful issuance of certificate
✓ Liability of subscriber to relying party when compromise of private key
Legal Presumptions

☑ Traditionally the relying party has burden of authenticating signer’s identity.

☑ “Electronic signature,” “digital signature,” other types of enhanced signatures

☑ Understanding burdens and presumptions

☑ Digital Signature Guidelines proposed new rebuttable presumption that the digital signature was signed by the subscriber named in the certificate issued by a CA
Legal Presumptions (cont.)

✓ Rebuttable presumption by legislation:
  – EU Mar 98 Draft Directive, Utah (95), 5 other U.S. States (1996-99), Germany (97), Italy (98), Spain (99)

✓ Rebuttable presumption allowed by regulation:
  – Canada Electronic Signatures Bill C-54

✓ Little or no effective presumption:
Legal Presumptions (cont.)

✓ Arguments FOR a legal presumption
✓ Arguments AGAINST a legal presumption
✓ Broad commercial use of PKI will not wait for the legislative outcome
✓ Absence of a legislative presumption will simply mean more business for trial lawyers until a judicial presumption emerges.
Evidentiary coverage

✓ What is a signature?
✓ Elements? (e.g. public key, signature, CRL, time and date stamp)
✓ Extrinsic evidence involving the facts and circumstances of the transaction?
✓ Expert testimony as foundation
Incorporation by reference

- Technical limitations of size of certificate
- Publication of terms (ETERMS repository)
- Incorporation of legal terms (CP)
- Notification (end user software)
- Legal limitations (civil/common law)
Related Activities

✔ ETERMS Project
✔ Certification Services Agreements and Model Clauses
✔ PKI Industry Association
ETERMS Notices/Disclosures

✓ Practice variations becoming obstacle to the growth of global electronic commerce
✓ ETERMS provide market-based solution to inconsistent notice/disclosure terminology
✓ Initial application will be between commercial entities
✓ Result: harmonize the implementation of notices/disclosures in end-user applications
Relationship Models

✔ Open/Unbounded Models
  – CA ↔ Business
  – CA ← → Consumer/Individual

✔ EDI / Existing Relationships to PKI (Addendum)
  – Business ↔ Business over a PKI
Relationship Models (cont’d)

✔ Privity Models
  – [CA ↔ Bus] ↔ Consumer
  – CA ↔ Business ↔ [Business or Consumer]

✔ Non-transactional / communication model
  – Individual ↔ Individual over a PKI
Global PKI Industry Association

✔ General education
✔ Promotion of self-regulation
✔ Policy development and advocacy
✔ Develop and advance industry practices
Wrap up

✓ Liaisons (who else?)
✓ Harmonization or unification?
✓ Collaboration: next steps