23rd NISSC, Baltimore - Oct 2000

Achieving Global Trust in an e-World

Richard Wilsher

the Σygma partnership

RGW@Zygma.Co.UK
+44 12 45 40 15 24

Why do we need Global Trust in an e-world?

- Increasingly, Internet is the vehicle for commerce;
- Increasingly, commerce is cross-border;
- Volume of intangible trade is increasing;
- Proportion of SMEs participating is increasing;

Why do we need Global Trust ……… ?

- The value of transactions will increase;
- The cost of failure will correspondingly go up;
- The requirement for trust, confidence, security is **fundamental** to enable:
  - more sophisticated use of the Internet;
  - more widespread use of the Internet.
- Technology *per se* is not the solution

Seamless Trust - some objectives:

- actively encourage innovation and the growth and development of electronic business;
- encourage the development of new ways of conducting electronic business, and of providing privacy and trust;
- provide a range of services which appear to the subscriber as an integrated, seamless whole;

the Σygma partnership

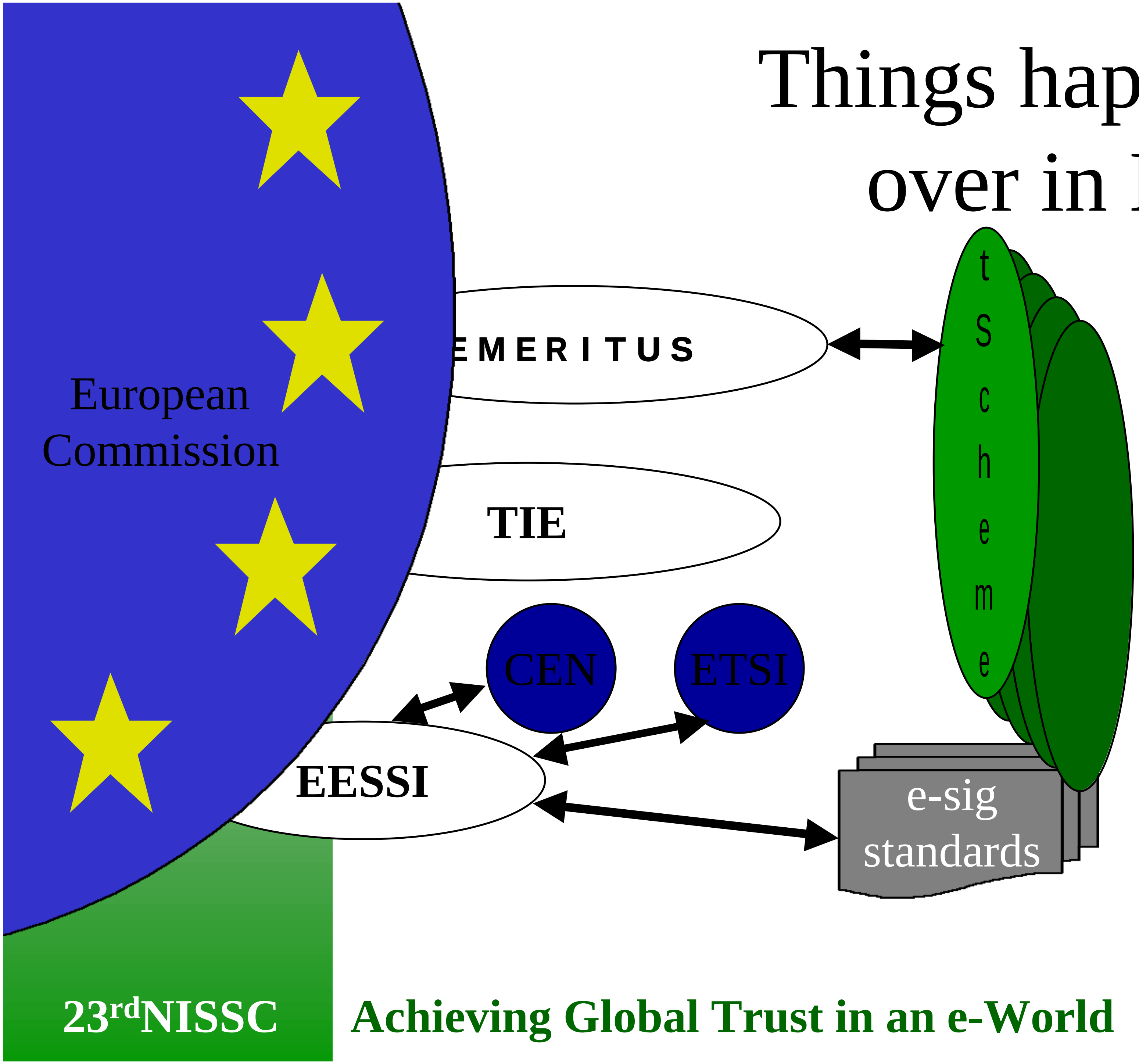
…... some more objectives:

- conform everywhere to international trade principles;
- not to threaten any nation's sovereignty, security or economic well-being;
- co-operate with governments, acknowledging their concerns associated with certain uses of cryptography;
- achieve a policy approach that will apply in all developed and developing economies Worldwide.

What is the basis for Global Trust?

- Common standards:
  - – technical;
  - – non-technical.
- Common business practices & criteria;
- Equivalent assessment processes & requirements for evidence;
- Equivalent strength / rigour (and hence assurance).

Things happening over in Europe



EMERITUS - Goals

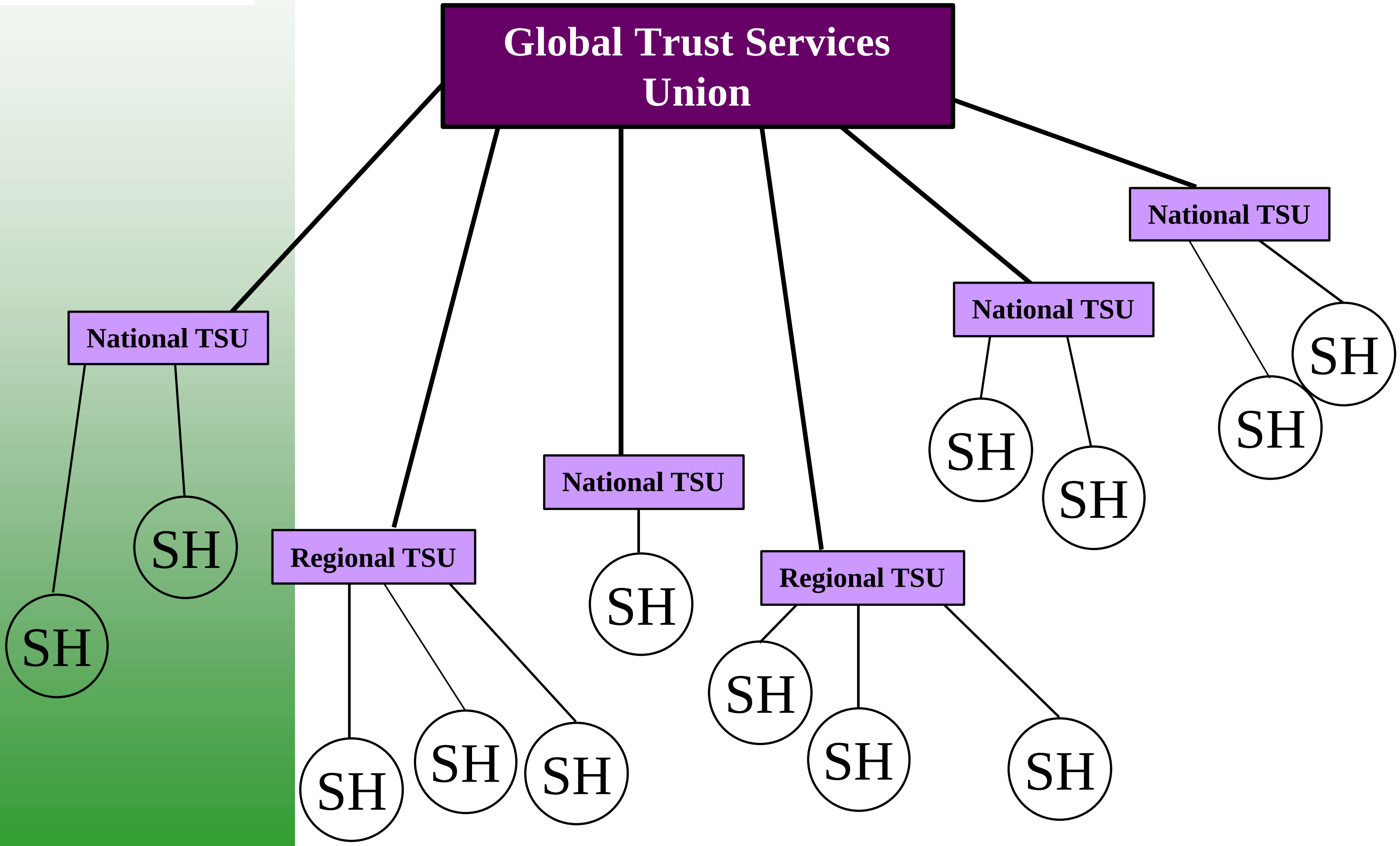
E-*business* **M***odel for the* **E***ffective* **R***eal***I***sation of a* **T***r***U***st* **S***ervices infrastructure*

- Industry-led co-regulation;
- Creating a Global Trust Services Infrastructure;
- Agreeing a common approach to assessing TSPs;
- EC funded project (€ 330,000), led by FEI (UK).

EMERITUS - StakeHolders

- All aspects of the marketplace, industry and government involved:
  - Users (through business and user associations, groups);
  - Trust Service Providers (through associations and individually);
  - Technology suppliers (through associations and individually);
  - Governments and Regulators.

EMERITUS - concept



Established TSUs

UK	tScheme
SP	AECODI
NL	TTP.NL
AT	A-SIT
IT	??
FI/NO/SE ??	

tScheme - status

- Registered limited company, under English law;
- Not-for-profit organisation;
- Funded initially by its founder-members;
- Will transition to revenue-derived funding;
- Will co-operate with other like organisations.

tScheme - functions

- Definition / selection of Approval Profiles, operational & technical standards;
- Definition of the Approval process;
- Granting of approvals to applicant TSPs;
- Review / Renewal / Revocation / Mediation;
- Support for setting up of TSs;
- Promotion of approved Trust Services;

BUT (take note): No actual provision of TSs.

tScheme - where are we now?

- Approval Profiles:
  - defined for: Issuing Qualified Certificates;
  - Issuing Non-Qualified Certificates;
    Key Recovery;
    Time-Stamping.
- Recognised Certification Bodies;
  - ……..
- Pilots just completed.

Broader collaboration

- Already working with: AT, DE, IT, NL, SP;
- Discussions with many other EEA States
- Interest from: AUS, USA, CH, CZ, TR,
  - These all need to be strengthened.

Achieving Global Trust in an E-World

Michael S. Baum, J.D., M.B.A., CISSP

michael@verisign.com

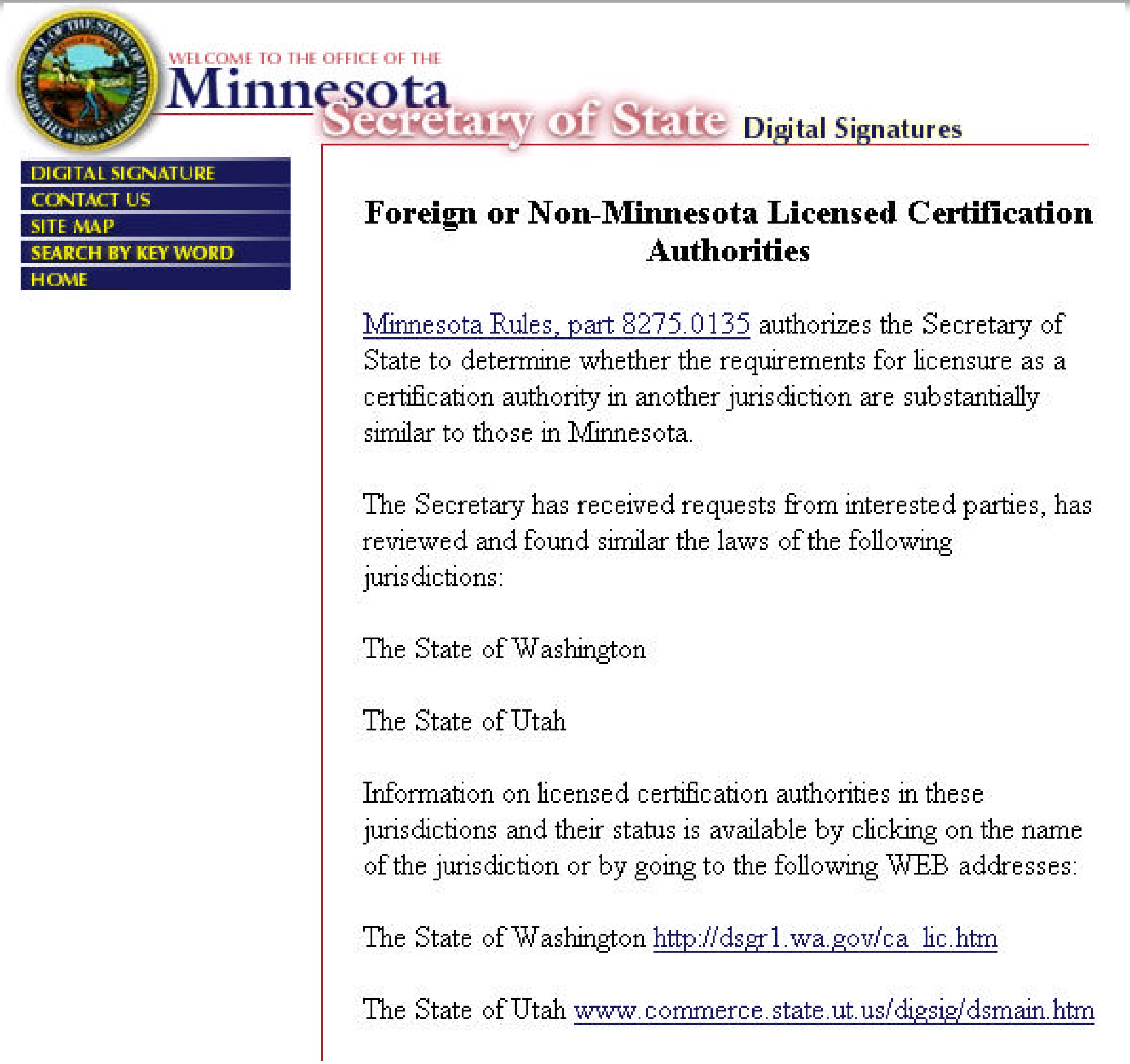
Interoperation Challenges

- ❑ Policy difficulties
- ❑ Learning curves
- ❑ Technology-neutral law
- ❑ Monolithic approaches
- ❑ Embryonic state of the industry
- ❑ Uneven implementation standards
- ❑ Lack of standardized CA quality metrics
- ❑ Difficulties in developing criteria for CA assessment
- ❑ Inadequate international and domestic law
- ❑ Insufficient technical solutions

Interoperation

- **Cross-certification**: Any situation in which a CA technically issues a certificate to another CA, regardless of the surrounding structure of CAs and regardless of whether one or multiple organizations are involved. Thus cross-certification can exist even within a chain that is entirely within a single domain or organization.
- **Interdomain certification:** Where a CA in one organization's domain issues a certificate to a CA in another organization's domain.

U.S. State Government Initiative



Foreign or Non-Minnesota Licensed Certification Authorities

Minnesota Rules, part 8275.0135 authorizes the Secretary of State to determine whether the requirements for licensure as a certification authority in another jurisdiction are substantially similar to those in Minnesota.

The Secretary has received requests from interested parties, has reviewed and found similar the laws of the following jurisdictions:

The State of Washington

The State of Utah

Information on licensed certification authorities in these jurisdictions and their status is available by clicking on the name of the jurisdiction or by going to the following WEB addresses:

The State of Washington http://dsgr1.wa.gov/ca_lic.htm

The State of Utah www.commerce.state.ut.us/digsig/dsmain.htm

The PKI Assessment Guidelines (PAG)

- ❑ A multidisciplinary initiative to develop objective guidelines to facilitate assessment of PKI interoperation and quality
- ❑ A logical extension of the Digital Signature Guidelines
- ❑ A legal framework for assessing both PKI products and managed services
- ❑ Guidelines *not* criteria
- ❑ A rich interdisciplinary educational resource valuable to specialists and neophytes
- ❑ Non-sectoral, cross-industry
- ❑ Guidance for drafting and assessing relevant PKI documents (e.g., CPs, CPSs, RPAs)
- ❑ A *living treatise*

Some Underlying Guiding Principles

- ❑ Legal validity *and* enforceability
- ❑ PKI trustworthiness, accountability and certainty
- ❑ Interoperation, recognition and nondiscrimination
- ❑ Facilitation of e-commerce
- ❑ Freedom of contract
- ❑ Protection of consumers
- ❑ Public policy conformance

PAG Substantive Outline

Section 1. INTRODUCTION

Section 2. GENERAL, LEGAL, & BUSINESS PROVISIONS

Section 3. VALIDATION OF IDENTITY AND AUTHORITY

Section 4. CERTIFICATE LIFE CYCLE OPERATIONAL REQS.

Section 5. CA FACILITY AND MANAGEMENT CONTROLS

Section 6. TECHNICAL SECURITY CONTROLS

Section 7. CERTIFICATE AND CRL PROFILES

Section 8. SPECIFICATION ADMINISTRATION

Some Standards Considered

- ❑ **General Usage for International Digitally Ensured Commerce (GUIDEC)**
- ❑ **RFC 2527: Internet X.509 Public key Infrastructure – Certificate Policy and Practices Framework**
- ❑ **BS 7799-1:1999: A Code of Practice for Information Security Management**
- ❑ **Standard Qualified Certificate Policy for Certification Service Providers Issuing Qualified Certificates**
- ❑ **Federal Information Processing Standard Publication 140-2**
- ❑ **AICPA/CICA WebTrust Principles and Criteria for System Reliability**
- ❑ **X9.79: Public Key Infrastructure - Practices and Policy Framework**

Conformance to Developing Global Practices and Standard

Model Law on Electronic Commerce

CyberNotary & PKI Industry Assn.

Guidec & ETERMS

PKIX - RFCs

Certificate Management Control Objectives

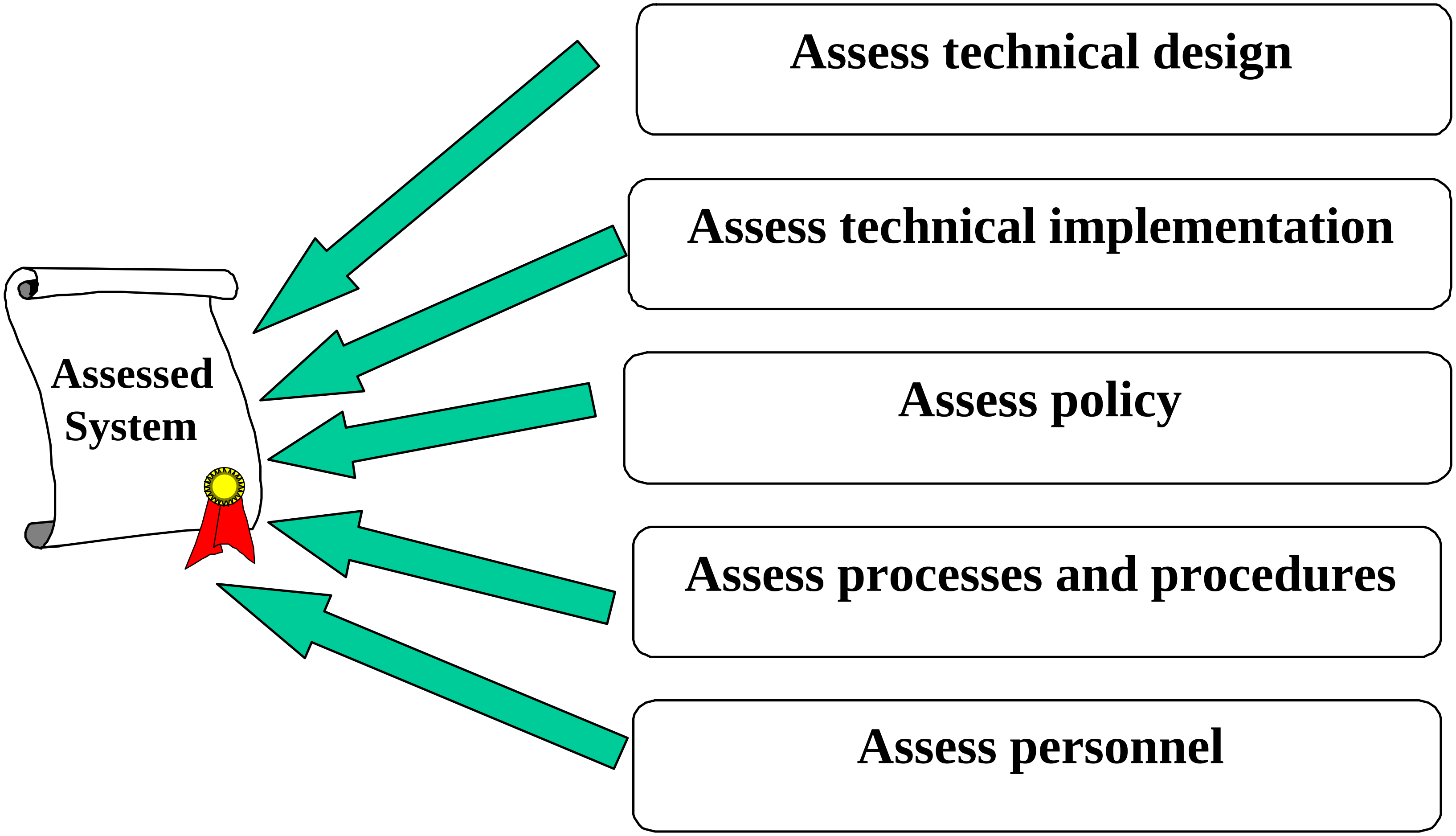
Privacy Policy

Authentication Studies

Electronic Signature, Privacy and Ecommerce Directives

PKI Assessment Guidelines & Digital Signature Guidelines

Assessment Components



Assess technical design

Assess technical implementation

Assess policy

Assess processes and procedures

Assess personnel

Some US State CA Licensing/Approval Regimes

California

Minnesota

Nebraska

North Carolina

Oregon

Texas

Utah

Washington

Trustworthy PKI Requirements and Commercial Realities?

EU – E-Signature Directive

Australia – Gatekeeper

Germany – Digital Signature Law

Italy – Digital Signature Law

CLARITY - MAPPING - COST

United Nations Commission on International Trade Law

UNCITRAL

Working Group on Electronic Commerce

- **UN Model Law on Electronic Commerce (1996)**

  Basic facilitation and *technology neutrality*

- **Draft Uniform Rules on Electronic Signatures**

UNCITRAL Model Rules: Gap Fillers?

- ❑ **Subscribers:** **"Each signature holder shall … exercise reasonable care to avoid unauthorized use of its signature device."**

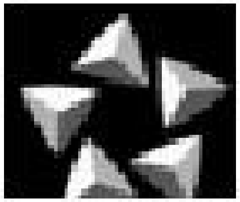
  Partial Proposed Art. 8

- ❑ **Relying Parties:** **"A person is not entitled to rely on an electronic signature to the extent that it is not reasonable to do so."**

  Partial Proposed Art. 12

Composite Assessment & Trust Marks

- Modeled on the airline industry's *Star alliance*
- Responds to a proliferation of trust marks
- Modular and flexible – assessment components could include:
  - Information systems (server and client systems)
  - Cryptomodules / key management
  - Policies and practices
  - Privacy
  - Business practices
  - Personnel professional credentials
- Encourages assessor competition



Multi-State
Digital Signature Summit: Post Mortem

- ❑ An effort to pool the collective expertise of state policy executives and technology experts and identify ways to remove barriers to the implementation of digital signature technology
- ❑ Considering-
  - ➢ Federal pre-emption of State D.S. rules
  - ➢ Foreign recognition of certificates/signatures
  - ➢ Harmonizing accreditation for CA licensing
- ❑ August 10 – 11 in San Francisco
- ❑ Sponsored by the Cal. Secretary of State

VeriSign™

PDS

Model PKI Disclosure Statement

- CA contact information
- Certificate type, validation procedures and usages
- Reliance limits
- Obligations of subscribers
- Certificate status checking obligations of relying parties
- Limited warranty & disclaimer/ Limitation of liability
- Applicable agreements, CPS, certificate policy
- Privacy policy
- Refund policy
- Applicable law and dispute resolution
- CA and repository licenses, trust marks, and audit