



DocuSign®

PKI-Форум Россия 2011

Доктор **Кен Мойль** (Ken Moyle), директор по правовым вопросам компании DocuSign, США

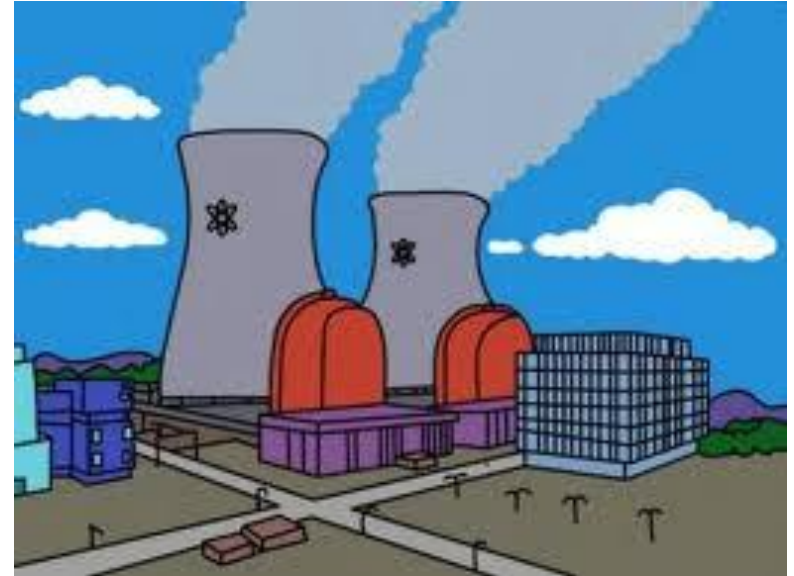


Millions of business transactions

- Many types
 - Simple vs. complex
 - High vs. low value
- Varying levels of business risk
 - Repudiation – what is the likelihood? The value?
 - Fraud – how can the situation be abused?
 - Mistake – how complex is the transaction? Is there a consumer involved?



“Sliding Scale” of Risk Mitigation



Written Agreements

- Legal requirement
- Business Tradition
- Facts and circumstances (risk mitigation)

Identifying the signatory to an agreement

- Face to face
- Known party
- Known mailing address
- Notary



Identifying the signatory to an agreement

- ✓ Face to face
- ✓ Known party
- ✓ Known mailing address



- *Evidence*
- *Proof*

Electronic agreements



No such thing as perfection

- Directive 93/1999 EC focus on Qualified Electronic Signature (Advanced Electronic signature + Qualified Certificate)
- No real attention on “simple” electronic signature for simpler transactions that do not require the highest levels of authentication
- High security, but low adoption at high cost
- Paralysis of business-to-business (B2B) and business-to-consumer (B2C) use of electronic signatures in commerce due to confusion about legal enforceability

A signature is not identification

A. Maichez



A signature is not identification



Paper Slows the Speed of Business



Fax Machines...



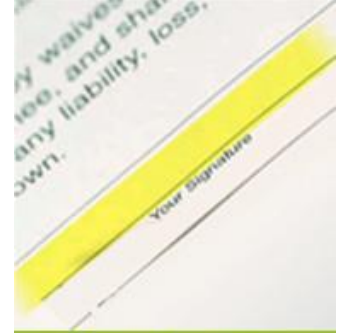
Printing to Sign...



Wait for Overnight Express...



Lost Paper Contracts...



Missing Signatures...



Distribute Copies to Each Signer...

eID Initiatives in Other Countries

- Varying stages of development
- Mixed results, varying approaches
- Examples
 - Canada
 - Australia
 - United States

eID Initiatives in Other Countries

- Canada
 - 2007 Task force to recommend a pan-Canadian Identity Management and Authentication (IdM&A) Framework
 - 2011 – Treasury Department outlined its “incremental approach” to federated idM.
 - Collaboration with federal, provincial, and territorial partners;
 - Building trust through exploration of options for trust models;
 - Federating technology-neutral credentials; and
 - Developing an Identity Assurance Model
 - No timeline

No PKI requirement imposed on e-commerce



eID Initiatives in Other Countries

- Australia
 - National Identity Security Strategy (NISS) 2005
 - Identity Management for Australian Government Employees Framework (IMAGE) 2006
 - Australian Government e-Authentication Framework for Individuals (AGAF(I)) 2006
 - eGovernment only
 - Dept. of Immigration & Citizenship
 - idM for controlling immigration

No PKI requirements imposed on e-commerce



eID Initiatives in Other Countries

- United States
 - National Standard for Trusted Identities in Cyberspace (NSTIC) – “Identity EcoSystem”
 - Federated, not centralized
 - Private trusted ID providers, not government
 - Few technical standards imposed
 - Exceptions: FICAM, NIST SP 800-63, GFIPM, FIPP
 - distrust, privacy issues driving approach
 - Electronic Medical Records
 - No PKI requirement imposed on e-commerce



eID Initiatives in Other Countries

- Common themes:
 - A federated approach, leveraging public-private sector cooperation
 - Technology neutrality, allowing for current and emergent technologies to enhance eID programs by continuing to compete and innovate



Promote, improve, adopt PKI, but...

- Accept alternative forms of authentication/identification, to match the risks of the transaction
- Allow parties to a transaction to decide the level of risk to accept
- Consider technology neutrality
 - In legislation and rulemaking
 - In the legal community
- Know that citizen adoption of e-signature will require flexibility

