Deloitte.

Current Initiatives in Global PKI
Establishing Trust in Public and Private Sectors

Donald E. Sheehy, CA*CISA, CRISC, CIPP/C

Associate Partner

This session will discuss

- Brief introduction of Public Key Infrastructure (PKI)
- PKI as a key component in deployment of electronic commerce
- Key players in PKI
- Examples of government deployments
- Risks and issues
- New standards for trust in PKI

What is PKI

- PKI stands for **Public Key Infrastructure**
- Architecture designed to proof the identities of people, web sites, computer programs, etc. on the Internet.
- In a PKI, a **Certificate Authority** (CA) issues **Digital Certificates** to applicants. The CA also verifies the identity of applicants, and publishes certificates on an on-line repository where people can lookup others' certificates.

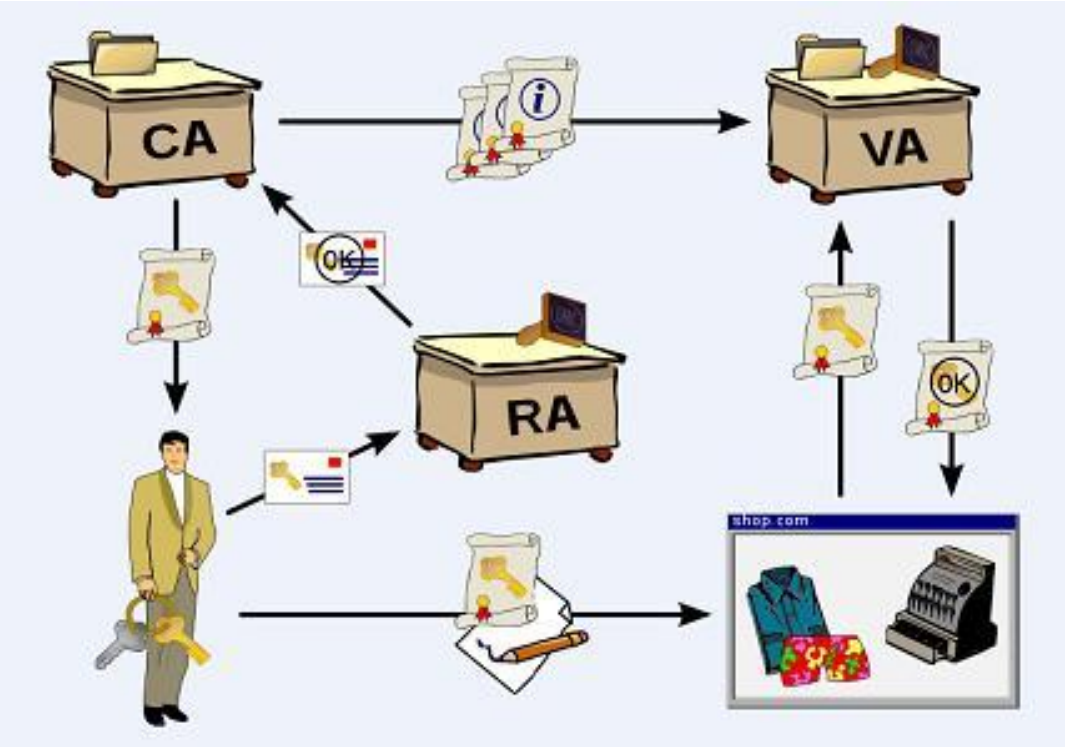
Why PKI

- A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.
- The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates

How does PKI work

- PKI uses public/private-key pairs–two mathematically related keys (asymmetric cryptography)
- One of these keys is made public, by posting it on the Internet for example, while the other remains private.
- Public-key cryptography -a message encrypted with the public key can only be decrypted with the private key, and, conversely, a message signed with a private key can be verified with the public key.
- This technology can be used in different ways to provide the four ingredients required for trust in e-commerce transactions: confidentiality, authentication, integrity, and nonrepudiation.

Illustration



- A user applies for a certificate with public key at a registration authority (RA).
- RA confirms the user's identity to the certification authority (CA) which in turn issues the certificate.
- The user can then digitally sign a contract using the new certificate. Identity is then checked by the contracting party with a validation authority (VA) which again receives information about issued certificates by the CA

PKI

- A transaction submitted by a customer to an online merchant via the Internet can be encrypted with the merchant's public key and therefore can only be decrypted by that merchant using the merchant's private key—ensuring a level of confidentiality.
- Confidentiality can also be achieved through the use of Secure Socket Layer (SSL), Secure/Multipurpose Internet Mail Extensions (S/MIME), and other protocols, such as Secure Electronic Transaction (SET).

Who are the Key Players

- Public Certfication Authorities
- Browsers
- Users
  - Financial insitutions
  - Manufacturing
  - Public Sector

Certification Authorities

netcraft.com, top certificate authorities in 2009 are:

- 21.17% Go Daddy GoDaddy.com, Inc.
- 12.79% VeriSign Equifax Secure Inc.
- 11.19% VeriSign Thawte Consulting cc
- 10.58% Comodo UTN-USERFirst-Hardware
- 8.23% VeriSign VeriSign, Inc.
- 7.80% VeriSign Equifax
- 6.38% VeriSign VeriSign Trust Network
- 3.37% Comodo Comodo CA Limited
- 2.55% Network Solutions Network Solutions L.L.C.
- 2.25% Go Daddy Starfield Technologies, Inc.
- 1.57% DigiCert Inc
- 1.33% Entrust.net Entrust.net

Browser Market Share

Browser	Global March 2010	Global March 2011	SA March 2010	SA March 2011
Microsoft IE	54.44%	45.11%	56.38%	47.22%
Firefox	31.27	29.98	31.66	26.21
Google Chrome	7.29	17.37	10.25	25.0
Safari	4.16	5.02	0.81	0.93
Opera	1.97	1.97	0.74	0.55
Source – Statcounter.com				

Users - Financial Institutions

- (NIST) PKI It enables both encryption and non-repudiable digital signatures, which offer stronger integrity and confidentiality than are possible with traditional paper.
- Many applications
  - replacement of paper documents and paper based services
  - mutual authentication of previously unknown parties for electronic transaction, while protecting the confidentiality and integrity of the transactions. This can be done over otherwise insecure networks.

Users - Financial Institutions

- Create operation efficiencies
- Need to use PKI to participate effectively in electronic commerce.
- May also choose to offer PKI services to the public, as a business line in its own right.

Financial Institution Example

- Many financial institutions now offer online services to their customers over the Internet.
- Institutions often have secure webservers that use the SSL protocol with a server certificate to establish an encrypted link for the banking service.
- The customer is usually authenticated with a PIN.
- A few financial institutions are now issuing certificates to customers to use for online banking.
- The SSL protocol can use a client certificate to authenticate the client to the server. This method offers stronger customer authentication than a PIN.

Financial Institution Example

- In most cases, certificates are strictly for use with the issuing institution.
- Since these applications generally plug into and require an online system with access to account information, certificate revocation is handled automatically.
- There may not be any information about the customer except an account number in the certificate. Everything else is available through access to account information.
- The business model is very simple, because the issuer and the relying party are the same institution.
- The primary barrier to the use of customer PKIs is current PKI clients. They are not as user friendly and as mature as they need to be to allow ordinary customers to be comfortable getting, managing, and using their certificates.

SET

- The Secure Electronic Transaction (SET) protocol combines a special purpose PKI with the existing credit card infrastructure to allow more secure use of credit card services over the Internet.
- This goes beyond a single financial institution, but its use is still limited to credit card transactions.

Manufacturing - Airlines

- Airbus 380 – SITA uses PKI for suppliers for Airbus 380. All suppliers need to be authenticated through LRAs for inclusion.
- Boeing 787 - Boeing uses the Public Key Infrastructure (PKI) for exchange of encrypted email. These keys are contained in the user's public and private X.509 user certificates. Anyone who has a copy of a user's public certificate can encrypt email that only the certificate's owner can decrypt using their private certificate.

Government – a few examples

- Canada
- United States
- Saudi Arabia
- Australia

Government - Canada

- A key initiative has been the establishment of the Government of Canada Public Key Infrastructure
- PKI strategy goal is the establishment of a secure federal electronic service delivery system based largely on a centrally managed Public Key Infrastructure cross-certified with other PKIs.
- Internal Credential Management operates and maintains the CA, which is a trusted third party responsible for issuing digital certificates.

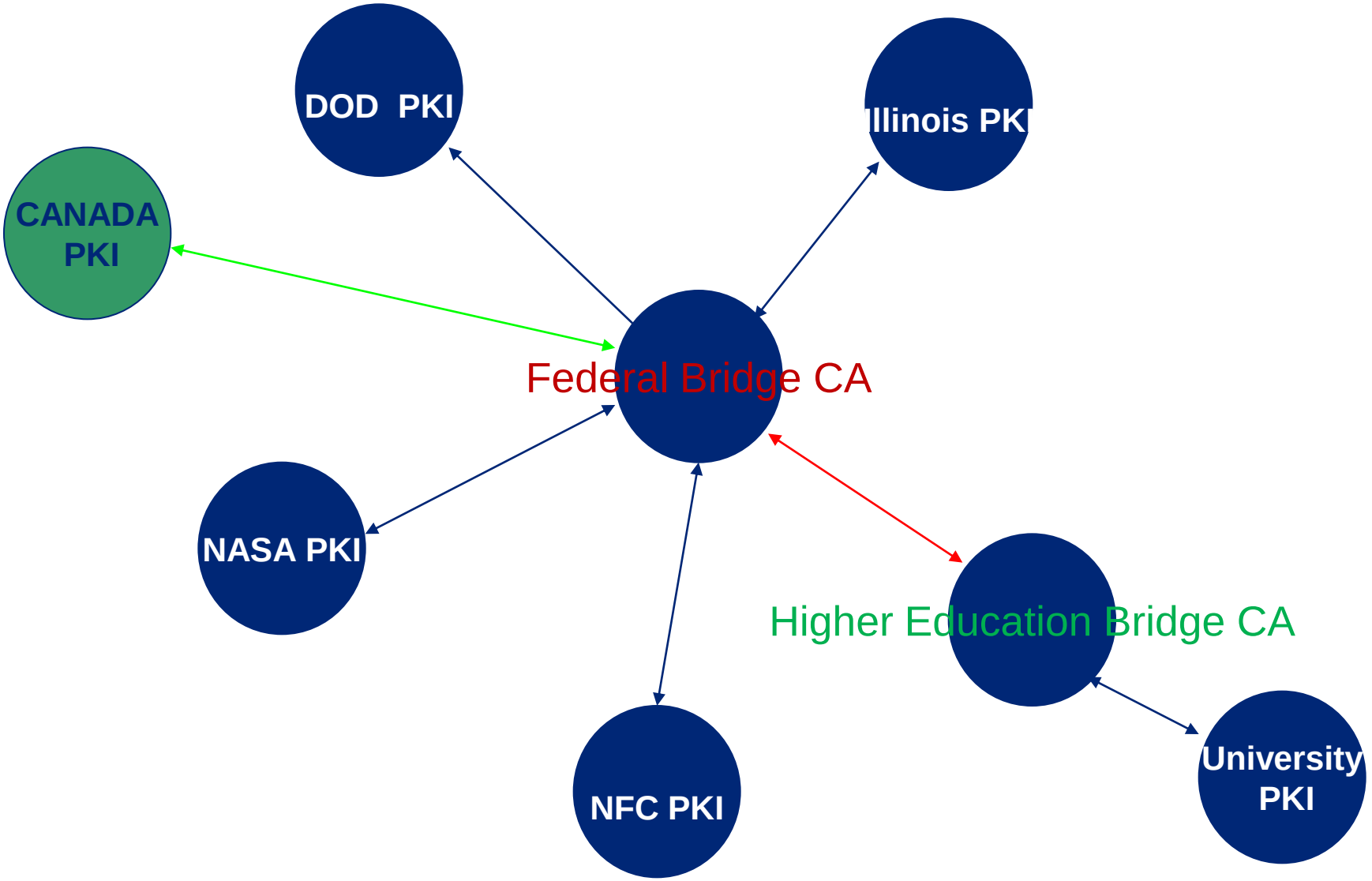
Government - Canada

- A federal department may operate its own Certification Authority, or choose to enter into a contract with another organization for the provision of Certification Authority services,
- Departmental Local Registration Authorities(LRAs) or the Online Registration and Credential Administration (ORCA) system ensure that the individuals or organizations applying for granted digital certificates or **MyKey** are, in fact, whom they claim to be.
- Online Registration and Credential Administration (ORCA) is an online system that enables users to securely create and manage their PKI identity-based credential (**MyKey**).

U.S. Federal PKI

- Agencies implement their own PKIs
- Create a Federal Bridge CA using Customizable Off The Shelf products to bind Agency PKIs together
- Establish a Federal PKI Policy Authority to oversee operation of the Federal Bridge CA
- Ensure directory compatibility
- Use Access Certificates for Electronic Services for transactions with the public

A Snapshot of the U.S. Federal PKI



Saudi Arabia

- Kingdom of Saudi Arabia has created a National Public Key Infrastructure, named the National Center for Digital Certification (NCDC).
- Authentication, Digital Signature, Encryption and non-repudiation services for access and processing of electronic information, documents and transactions.
- NCDC provides trust services to secure the exchange of information between key stakeholders. Participants include:
  - Government
  - Citizens
  - Business

Saudi Arabia

- The NCDC operates as a closed business system model.
- It uses Digital Certificates issued by Certification Authorities (CAs) meeting rules established by the NCDC's governing body the National Policy Authority (NPA).
- The NCDC owns and operates the Root Certification Authority of the Kingdom of Saudi Arabia.
- Approved Certification Authorities (CAs) shall be issuers of NCDC Digital Certificates to Subscribers, Relying parties and Registration Authorities
- Together all of these components and participants form the "Saudi National PKI."

Saudi Arabia

- A new service delivery model has been created whereby a shared National PKI Center has been created.
- The National Center for Digital Certification - Shared Services Center (NCDC-SSC) will host CAs and manage operations for CA's joining the Saudi National PKI.

Australia

- Gatekeeper is the Australian Federal Government's initiative for digital certificates
- There are a number of Federal and State Government Agencies which have made their services available online to those using Gatekeeper digital certificates.
- Need for accreditation
- The information an organization requires to obtain or maintain Gatekeeper Accreditation has been arranged to distinguish between the types of Accreditation available under Gatekeeper CA and RA

Risks and Issues Faced in PKI

- Inadequate security?
  - Security is a chain; as strong as the weakest link.
  - Security of any CA-based system is based on many links -not all cryptographic. People are possible security weaknesses as are computers
- Private Key Storage
- Strength of Identity checking
- RA issues

Standards

- Technical
- Control Framework
- Browser requirements
- Extended Validation

Technical

- Based on X.509 - defines what information can go into a certificate, and describes data format. All X.509 certificates have similar required data, in addition to the signature
- ANSI X.9 – Financial industry standards
- ISO – for example ISO/CD 21188 - Public key infrastructure for financial services -- Practices and policy framework

Technical

- PKIX standards _ RFC's govern most parts – for example
  - RFC3820 - Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile
  - RFC2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol –OCSP
  - RFC2527 then 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
  - RFC2511 - Internet X.509 Certificate Request Message Format
  - RFC2797 - Certificate Management Messages over CMS
  - RFC3039 - Internet X.509 Public Key Infrastructure Qualified Certificates Profile
  - RFC3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
  - RFC3281 - An Internet Attribute Certificate Profile for Authorization

Control Frameworks

- Number of frameworks
  - ETSI (European based)
  - ISO
  - Trust Services (WebTrust for CA)

Browser Requirements

- Require WebTrust or equivalent (ETSI allowed Europe)
- New technical requirements as a result of Comodo breach
- Require audits of RAs that can cause issuance of certs

CA Browser Forum

- http://www.cabforum.org/
- A voluntary organization of leading certification authorities (CAs) and vendors of Internet browser software and other applications.
- Members of the CA/Browser Forum have worked closely together in defining the guidelines and means of implementation for the Extended Validation (EV) SSL Certificate standard
- Consists of all major browsers and about 40 CAs across globe
- Setting new baseline standards for SSL at present