Certificates in the Internet: State, Issues, and Futures

Andrew Nash
Director, PKI Technologies and Standards
RSA Security, Inc.

RSA LABORATORIES

Presentation Scope

- **Understand status and directions of Internet certificate usage, from standards perspective**
  - **Certification infrastructure work**
  - **Application usage topics**
  - **Identify questions under discussion**
  - **What's coming next?**

RSA SECURITY

Where Does Internet Certificate Standards Work Stand?

- PKIX X.509 certificate profile and core protocols defined and largely stable
- Reference implementations distributed, interoperability testing performed
- Major applications adopting PKIX results
- Infrastructures and products being deployed
- Current PKI work emphasizing
  - enhancements
  - additional services
  - application integration

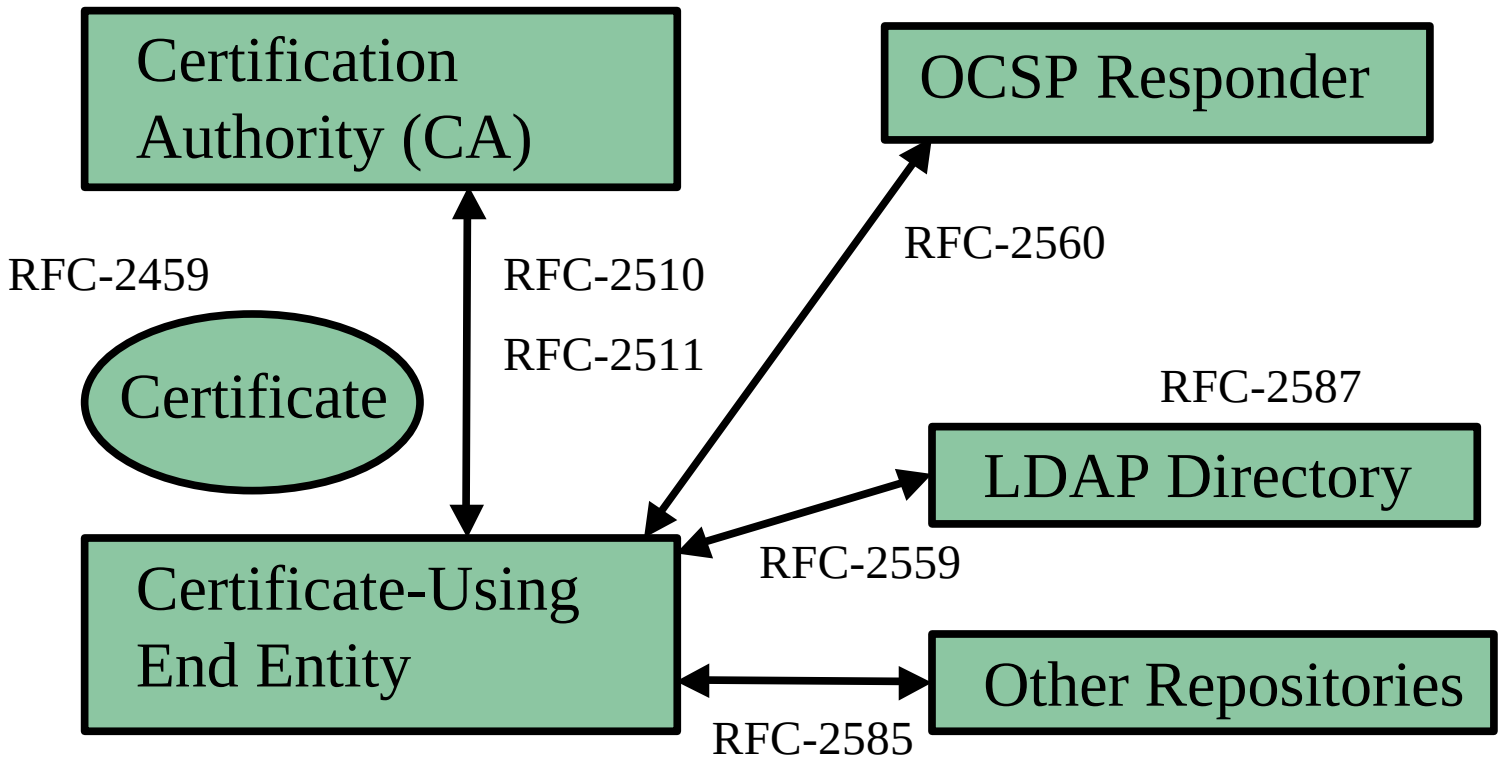
RSA SECURITY

IETF-PKIX Proposed Standards

- **1999 was a very busy year...**
- **Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459, January)**
- **Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510, March)**
- **Internet X.509 Certificate Request Message Format (RFC 2511, March)**
- **Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 (RFC 2559, April)**
- **Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP (RFC 2585, May)**
- **Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2587, June)**
- **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560, June)**

RSA SECURITY

Where the PKIX RFCs Fit



RSA SECURITY

Recent Active Topics

- Certificate Profile Issues
- Management Protocol Alternatives (CMP, CMC)
- Validation Protocol Alternatives (OCSP, DCS, SCVP, OCSP-X)
- Attribute Certificates
- Qualified Certificates
- Timestamping and Data Certification
- Application Integration (S/MIME, IPsec, LDAP)

RSA SECURITY

Profiling X.509 for Internet use: Some Aspects

- **Naming**
  - subjectAltNames containing Internet-form names
  - name constraint processing admits DNs, subjectAltNames, or both
- **authorityInfoAccess extension**
  - enables reference to named objects providing CA information and services, accessible via specified methods
  - enables linkage to non-CRL revocation data

RSA SECURITY

Algorithm Usage

- **RFC-2459 profiles certificate signatures:**
  - **for hash algorithm, SHA-1 recommended, MD5 and MD2 also recognized**
  - **for signatures, RSA or DSA**
- **RFC-2459 profiles certificates' subjectPublicKeys:**
  - **RSA**
  - **Diffie-Hellman**
  - **DSA**
- **RFC-2459 does not mandate use of the profiled choices, and allows other algorithms; additional profiling applied in per-application documents**

RSA SECURITY

Certificate Management

- **CMP (RFC-2510)**
  - **Workshops have verified cross-vendor interoperability**
  - **Some implementors' agreements were needed and discussed**
  - **Can layer over TCP, SMTP, HTTP**
  - **Incorporates CRMF formats**
- **CMC**
  - **"Certificate Management Messages over CMS" draft proposes alternative approach, layered on S/MIME work**
  - **Has passed PKIX WG Last-Call**
  - **Can carry CRMF, also supports PKCS#10 registration**

RSA SECURITY

Validation Approaches

- **Standards-track PKIX approaches:**
  - **CRLs: “traditional” PKI revocation checking method**
  - **OCSP: on-line query for revocation status**
- **Other working proposals providing on-line validation: DCS, SCVP, OCSP-X**
- **Issue: what validation elements to delegate from client to a central service?**
- **Issue: Which will work best in large operational environments?**

RSA SECURITY

More on CRLs

- **Full CRLs may grow large, incurring costs to propagate information where it's not needed**
- **Many facilities defined and discussed, usage models evolving**
  - **Delta CRLs: changes rather than full CRL; less transferred data, more processing complexity**
  - **CRL Distribution Points: certificate identifies its corresponding DP**
  - **CRL Scopes: CRL identifies the certificates it covers**
- **Revocation responsiveness limited (e.g., days)**

RSA SECURITY

More on on-line validation

- **OCSP provides on-line status query service**
  - **responder may be backed by CRLs or CA's repository, so MAY have faster responsiveness than CRLs**
  - **CA delegates authority to OCSP responder, which returns signed responses to queries**
  - **Core scope constrained to revocation status, but response extension facility available**
- **DCS, SCVP, and OCSP-X propose different sets of broader server-provided functionality, such as**
  - **path construction**
  - **path validation**
  - **data certification**

RSA SECURITY

Non-Repudiation

- Intent is to distinguish transactions (and accompanying certificates) with long-term accountability
- Legal frameworks are emerging
- PKI provides technical facilities supporting a broader service beyond the scope of PKIX standards
- Semantics, and relation between NR and other usage indicator bits within certificates, are contentious
  - PKIX profile allows NR bit to coexist with other key usage bits; not all X.509 profiles agree
- Qualified certificates, time stamping, data certification work items contribute to enhanced non-repudiation support

RSA SECURITY

Qualified Certificates

- **PKIX Qualified Certificates (QC) draft's goal is a further profile of X.509 certificates for personal authentication of human users**
  - **suitable for high assurance**
  - **suitable for legal recognition (e.g., EU directive)**
- **Naming attributes constrained for unmistakable identification of an individual; pseudonyms being incorporated**
- **User's QC could be placed on smart card; strong desire to serve multiple consuming applications**

RSA SECURITY

Timestamping

- **PKIX draft document specifies Timestamp Authority (TSA) service**
- **Systems requesting timestamps hash data objects, pass the hashes to TSA**
- **TSA uses reserved key to sign timestamps; corresponding certificate contains extendedKeyUsage identifying as TSA**
- **Patent issues are an identified concern for draft advancement**

RSA SECURITY

Data Certification

- **PKIX draft document defines Data Validation and Certification Server (DVCS), offering choice of services**
  - **Certification of claim of possession of data (hash of actual data presented); comparable to TSA service**
  - **Certification of possession of data (actual data presented)**
  - **Validation of digitally signed document**
  - **Validation of public-key certificates**
- **Returned validation certificate contains timestamped results**

RSA SECURITY

Attribute Certificates

- ISO Certificate Extensions (F)PDAM has extensive discussion of Attribute Certificates (ACs)
- Current activity in PKIX, with Internet AtttributeCertificate Profile for Authorization draft
- ACs linked to associated PKCs, chained to delegate access rights
- Usage will require integration into consumer protocols; accommodated for S/MIME, drafted for TLS

RSA SECURITY

Non-X.509 Certification Activities

- **Simple Public-Key Infrastructure (SPKI)**
  - SPKI Requirements, RFC-2692 (Experimental)
  - SPKI Certificate Theory, RFC-2693 (Experimental)
  - Uses S-expression syntax
  - Avoids global naming, emphasizes certified authorization
- **OpenPGP (OPGP) Message Format**
  - RFC-2440 (Proposed Standard)
  - Certification and cross-certification performed by users, not CAs
  - Key servers provide repositories to publish keys

RSA SECURITY

PKIX Adoption by Applications

- **PKIX-specified facilities are being profiled for operational use in applications, satisfying needs of those applications and their environments**
- **Tradeoff: application-tailored attributes and extensions vs. common, multi-use certificates**
- **Tradeoff: profiling by protocol vs. profiling by operational environment**

RSA SECURITY

Certificates in LDAP Directories

- **X.509's certificate-based authentication was originally defined for directory access purposes**
- **Today, LDAP provides a primary access method for PKI-related data within directories**
  - **PKIX-specified attributes and object classes represent basic security objects within schema**
  - **CAs provide certificates and CRLs for storage into attributes**
  - **Certificate users apply LDAP search and read operations to obtain needed objects**

RSA SECURITY

Certificate Usage: SSL/TLS

- **Secure Sockets Layer (SSL) widely used; Transport Layer Security (TLS) its standards-track successor**
- **Broad use of SSL server-side certificates**
  - **enables useful "secured pipe" from client to server, encapsulating HTTP and other protocols**
  - **number of certified entities is constrained**
- **Currently narrower usage of client-side certificates, client authentication**
  - **increased demand for client certification a driver for infrastructure growth**

RSA SECURITY

Certificate Usage: IPsec

- Core Internet Key Exchange (IKE) authentication modes are certificate-based
- PKIX Profile for IKE draft exists:
  - assumes certificate for device, not necessarily for user
  - extendedKeyUsage element designates IKE entities
  - some naming refinements, divergences from PKIX
  - does not mandate particular certificate enrollment mechanism
- Vendor interoperability workshops testing with certificates
- Some concerns about extending PKI to endpoints; interest in hybridizing with other authentication techniques

RSA SECURITY

Certificate Usage: S/MIME

- **S/MIME Version 3 Certificate Handling (RFC-2632) specifies additional procedures beyond PKIX**
  - **practices for sending and processing transmitted certificate sets and CRLs**
  - **support for E-mail address forms, usage of other extensions**
- **S/MIME Certificate Distribution Specification draft concerns publication in directories**
- **Special concerns include off-line determination of recipients' capabilities (e.g., supported algorithms)**

RSA SECURITY

Internet Certificates: Next Standardization Steps

- **PKIX Certificate Profile to Draft Standard, other documents to follow**
- **Progression and convergence on**
  - **management protocol alternatives**
  - **certificate validation alternatives**
  - **time stamping and data certification**
  - **qualified certificates**
  - **attribute certificates**

RSA SECURITY

Internet Certificates: Next Usage Steps

- **Lessons to learn as more applications integrate certificates**
  - **Usage models and profile elements will be validated or refined**
- **Lessons to learn as infrastructures scale to support more users**
  - **Operational experience will inform choices on certificate validation**
- **Broadening usage towards non-repudiation and authorization support**

RSA SECURITY