Use of X.509 in Internet Standards

Russ Housley

Past IETF Chair

Current IETF LAMPS WG Chair

Vigil Security LLC

9 May 2022

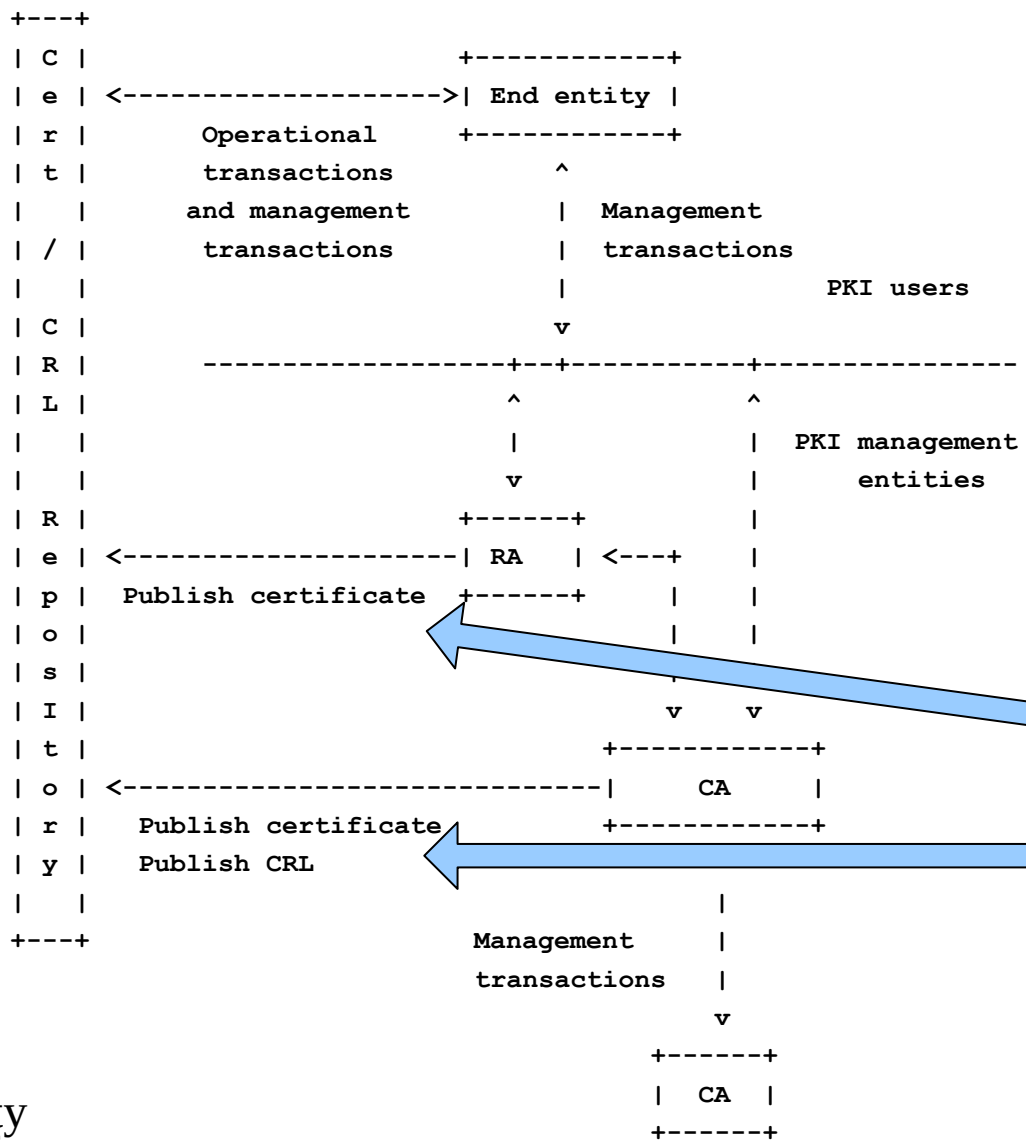
X.509: v1, v2, v3

- **CCITT X.509 (v1) published in Nov 1988**
  - X.500 Directory Authentication Framework
  - Privacy-Enhanced Mail (PEM) PKI [RFC1422] specification based on v1 in 1993; not deployed
- **ITU-T X.509 (v2) published in Nov 1993**
  - Adds two certificate fields for Directory access control
  - I am unaware of any v2 implementations
- **ITU-T X.509 (v3) published in Aug 1997**
  - Adds the extensions field to certificate and CRL
  - PKI using X.509 (PKIX) profile of v3 [RFC2459] in 1999; *very* widely deployed

IETF PKIX Working Group

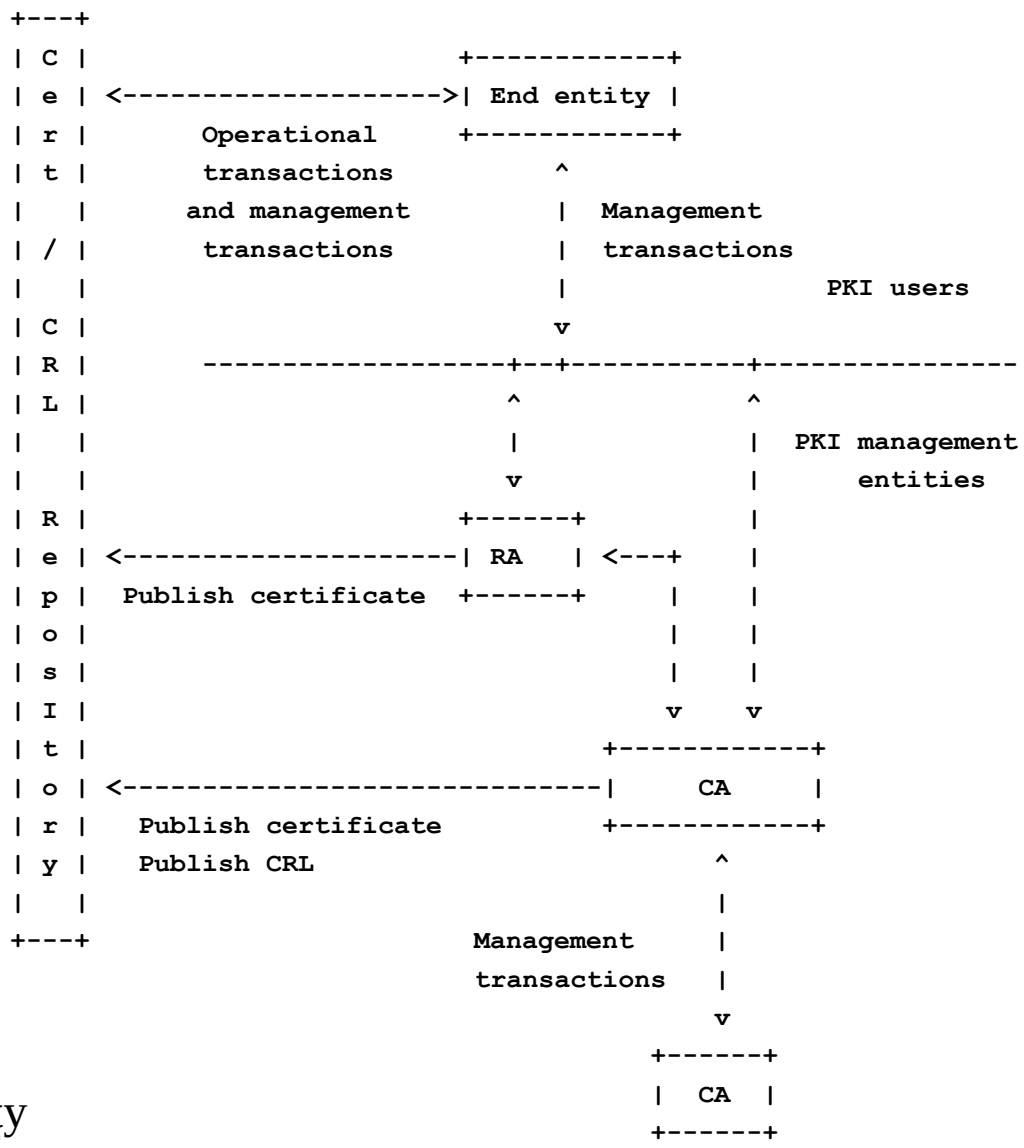
- Chartered in Oct 1995 to develop Internet standards to support X.509-based Public Key Infrastructures (PKIs)
- Profiled X.509 standards developed by the CCITT / ITU-T
- Independent initiatives to address X.509-based PKI needs in the Internet

PKIX Architecture



Vigil Security LLC

PKIX Architecture



IETF PKIX specified protocols to use and manage certificates and CRLs

Certificates and CRLs are defined in X.509

Vigil Security LLC

Early PKIX Vision

Initial view was four parts:

1. Certificate and CRL Profile [RFC2459]
2. Operational Protocols [RFC2559] [RFC2585] [RFC2587]
3. Certificate Management [RFC2510] [RFC2511] [RFC2797]
4. Certificate Policies [RFC2527]

However, X.509 was very widely accepted, and the effort grew, and in some cases, more than one way to do the same thing became standards …

PKIX: Oct 1995 to Oct 2013

PKIX WG published 70 RFCs:

- Certificate Profiles (PKC, Attribute, Qualified, Proxy, …)
- Operational Protocols
- Certificate Management (CMP, CMC, EST, …)
- Certificate Policies (CA, AA, TSA, …)
- Online Certificate Status Protocol (OCSP)
- Algorithm conventions (also proof-of-possession)
- Time-stamp protocol (TSP)
- Delegated of certification path construction and validation
- Trust Anchor Management Protocol (TAMP)
- Many certificate extensions and alternative name formats
- Informational specifications to aid implementers

LAMPS: Jul 2016 to present

Limited Additional Mechanisms for PKIX and SMIME

PKI-related RFCs:

- Updates and clarifications of PKIX RFCs
- Certification Authority Authorization (CAA)
- Additional algorithm conventions
- Additional certificate extensions
- Updates for Internationalization in names

Major upcoming work item:

- Post-Quantum Cryptography (PQC)

Protocols using X.509 Certificates

Many security protocols use X.509 certificates, including:

- TLS: Transport Layer Security
- IKE: Internet Key Exchange (IKEv1 and IKEv2)
- S/MIME: Secure Multipurpose Internet Mail Extensions
- JOSE: JSON Object Signing and Encryption
- COSE: CBOR Object Signing and Encryption

Many application protocols run on top of TLS or IPsec. Thus, many applications indirectly depend upon X.509 certificates, especially the world wide web.

Today, 1314 RFCs include “X.509” or “certificate”

Thank you!

Russ Housley
housley@vigilsec.com
+1 703 435 1775

Vigil Security LLC