v1.0 Nov 2012

Public Key Infrastructure © Aman Hardikar

Miscellaneous
- PKIX workgroup
  - http://datatracker.ietf.org/wg/pkix/charter/
- NIST PKI Program
  - http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/index.html
  - http://csrc.nist.gov/publications/PubsTC.html#PKI

Software
- Open Source / Free
  - OpenCA
    - http://www.openca.org/projects.shtml
    - Platform: [OS] Linux, Solaris, Mac
  - EJBCA
    - http://www.ejbca.org/
    - Platform: JEE
  - PHPki
    - http://phpki.sourceforge.net/
    - Platform: PHP (web based)
- Commercial
  - UniCERT
    - http://www.verizonbusiness.com/Products/security/identity/unicert/
  - Entrust Authority
    - http://www.entrust.com/pki/
  - RSA Digital Certificate Manager
    - http://uk.emc.com/security/rsa-digital-certificate.htm
  - Secure PKI
    - http://uk.safenet-inc.com/Solutions/Industry_Solutions_for/Secure_PKI/
  - KeyOne
    - http://www.safelayer.com/en/products-and-services/solutions/public-key-infrastructures
  - CoSign
    - http://www.arx.com/products/security-products
- Managed Service
  - Symantec / Verisign
    - http://www.symantec.com/en/uk/verisign/managed-pki-service
  - Entrust
    - http://www.entrust.com/managed_services/index.htm
  - Digicert
    - http://www.digicert.com/managed-pki-ssl.htm
  - Exostar
    - http://www.exostar.com/products-Federated_Identity_Service.aspx
  - Verizon
    - http://www.verizonbusiness.com/terms/us/products/security/managedPKI/
  - QuoVadis
    - http://www.quovadisglobal.co.uk/CertificateServices/ManagedPKI.aspx
- Bundled
  - Microsoft CA Services
    - Windows
    - Microsoft PKI Quick Guide
    - Building an Enterprise Root Certification Authority
  - FreeIPA
    - Linux (RedHat)
    - Includes DogTag Certificate System
    - http://www.freeipa.org/page/Main_Page

Audit Checklist
- Refer PKIAuditing Mindmap

Architecture Weaknesses
- Revocation: CRLs
  - Designed for X.500 and not web
  - Blacklist instead of whitelist
  - Revocation of root certificates
  - Size and distribution
  - Historical revocation status
  - Aggregation problem - privacy and maintenance
  - Delegation problem - restrictions on sub-CAs
  - Federation problem - complex and expensive validation
- Revocation: OCSP
  - CA
    - Certificate costs
    - Expiration date
    - Revocation issues
  - Implementation

Applications
- SSL
- S/MIME
- PEM
- PGP
- WLAN
- IKE

X.509 Certificate
- Standards
  - RFC5280
- Contains
  - Version
  - Serial Number
  - Signature Algorithm
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Information
    - Algorithm
    - Key
  - [Optional] Issuer Unique Identifier
  - [Optional] Subject Unique Identifier
  - [Optional] Extensions
    - Critical
    - Non-critical
  - Certification Authority's Digital Signature
    - Algorithm
    - Key

Simple Distributed Security Infrastructure (SDSI)
- Simple public-key infrastructure
- Standards
  - RFC 2692
  - RFC 2693

Key Management
- Generation
- Production
- Distribution
- Pre-production
- Post-production

Key States
- Pre-activation state
- Active state
- Deactivated state
- Destroyed state
- Compromised state
- Destroyed compromised state

Trust Models
- Subordinate Hierarchy
- Cross-Certified Mesh
- Bridge CA
- Trusted List

CRL Models
- Traditional CRL Model
- Modified CRL Models
  - Overissued CRLs
  - Segmented CRLs
  - Delta CRLs
  - Sliding Window Delta (Overissued Delta) CRLs
- OCSP - Online Certificate Status Protocol
  - OCSP Stapling

Protocols
- SCEP - Simple Certificate Enrollment Protocol — draft-nourse-scep-23
- MS-XCEP - X.509 Certificate Enrollment Policy Protocol
- CMP - Certificate Management Protocol — RFC 4210
- OCSP - Online Certificate Status Protocol — RFC 2560, 5019
- CMC - Certificate Management over CMS — RFC 5273
- SCVP - Server-based Certificate Validation Protocol — RFC 5055
- PRQP - PKI Resource Query Protocol
- TSP - Time-Stamp Protocol — RFC 3161

Kerberos Integration
- PKINIT - Public Key Cryptography for Initial Authentication — RFC 4556
- PKTAPP - Public Key Utilizing Tickets for Application Servers
- KX509 - Kerberized Certificate Issuance Protocol — RFC 6717
- PKCROSS - Public Key Cryptography for Cross Realm Authentication
- PKDA - Public-key based Kerberos for Distributed Authentication

Standards
- Certificate Request Message Format (CRMF) — RFC 4211
- Cryptographic Message Syntax (CMS) — RFC 5652, 5753, 5911
- Certificate and CRL Profile — RFC 3280
- Attribute Certificate Profile — RFC 3281
- IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX — RFC 4945
- Certificate Store Access via HTTP — RFC 4387
- PKIX RFC List — http://datatracker.ietf.org/wg/pkix/

PKCS Public Key Cryptography Standards

PKCS #1 RSA Cryptography Standard	RFC 3447
PKCS #3 Diffie–Hellman Key Agreement Standard	
PKCS #5 Password-based Encryption Standard	RFC 2898
PKCS #7 Cryptographic Message Syntax Standard	RFC 2315, 5652
PKCS #8 Private-Key Information Syntax Standard	RFC 5208
PKCS #9 Selected Attribute Types	RFC 2985
PKCS #10 Certification Request Standard	RFC 2986
PKCS #11 Cryptographic Token Interface	Cryptoki API
PKCS #12 Personal Information Exchange Syntax Standard	
PKCS #15 Cryptographic Token Information Format Standard	

Components
- Key Generater
- Key Management
- Certificate Authority
- Registration Authority
- Certificate Repositories
- CRL Distribution Points
- OCSP Service