D D S

PKI and storage of PGP and X.509 certificates in LDAP

LDAP Deployment BoF

Amsterdam 12.5.2000

Peter Gietz

Peter.gietz@directory.dfn.de

D D S

Agenda

- Why distribute public keys on Server?
- The classic: X.509
- IETF PKIX
- LDAP work on X.509
- PGP Keyserver
- A CA based Infrastructure for NRNs

D D S

Why distribute public keys on Server?

- Basics of any PKI
- Encrypt data for somebody without prior contact
- You don’t have to store all keys yourself
- Easier distribution of new keys and updates

D D S

Methods of key publication

- Without a third party:
  - own web page
  - via FTP file
  - via finger
- With a third party
  - dedicated key server
  - Directory

D D S

PKI and Directory

The Burton Group:

Network Strategy Report, PKI Architecture, July 1997:
(Quoted after: S. Zeber, X.500 Directory Services and PKI issues, http://nra.nacosa.nato.int/pki/hdocs/pkiahwg30/index.htm)

" ... Customers should always consider PKI a directory-enabled set of services and infrastructure. Without directory services, PKI will be exponentially harder to implement and manage. Consequently, customers should't deploy PKI widely without an accompanying directory plan"

D D S

Directory as Key Server

- Publishing medium for public keys and certificates
- Gets public keys from user
- Gets certificates from CA
- Documents revocation of keys/certificates (CRL)
- Documents status of a certificate at a specific time

D D S

X.509: The classic (1988)

- "The Directory: Authentication Framework"
- Part of the OSI-Directory standard X.500
- Defines Data model, e.g.:
  - userCertificate; cACertificate
  - crossCertificatePair
  - certificateRevocationList
- Defines mechanisms for authentification
- Certificate includes DN of the user
- Certificate includes DN of the signing CA

D D S

X.509v3 (1997)

- New extension mechanism
- Predefined extensions:
  - Information about key: identifier, usage, ...
  - Policy information: certificate policy, ...
  - User and CA extensions: alternative name, ...
  - Certification path constraints
- Lots of people see X.509v3 as independent from X.500
  - Problem: hypothetical DNs
  - No proof of uniqueness

D D S

X.509v4 (2000)

- Draft version ready (May 11, 2000)
  - ftp://ftp.bull.com/pub/OSIdirectory/4thEditionTexts/X.509_4thEditionDraftV2.pdf
  - Press release: http://www.itu.int/ITU-T/itu-t_news/sg7_x509_press.htm
- Includes verification of certificate chains with CAs from different domains and hierarchies
- Enhancements in the area of certificate revocation
- New features in attribute certificates (AC)
- Defines usage of ACs for access control and authorization

D D S

Applications of X.509 certificates

- Certificate based security on different levels:
  - Network Layer:
    - IPSec (Internet Protocol Security)
  - Transport Layer:
    - SSL (Secure Socket Layer) =
    - TLS (Transport Layer Security)
  - Application Level:
    - S/MIME (Secure Multipurpose Internet Mail Extensions) v3: patent free algorithms, mailing list support
    - PGP (Pretty Good Privacy), since version 6

D D S

IETF WG PKIX

- Defines an Internet PKI on basis of X.509 certificates
- Supports the following IETF security protocols:
  - S/MIME
  - TLS (=SSL)
  - IPSec
- Status:
  - 9 RFCs
  - 21 Internet Drafts
  - Overview: Arsenault, A. (DOD), Turner, S. (IECA), Internet X.509 Public Key Infrastructure PKIX Roadmap, <draft-ietf-pkix-roadmap-05.txt>, March 2000

D D S

PKIX and Certificate profiles

- **RFC 2459: Housley, R. (Spyrus), Ford, W. (Verisign) et.al., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999**
  redrafted:
  <draft-ietf-pkix-new-part1-01.txt>, March 2000
  defines:
  - **Certificate (X.509v3 standard fields and standard extensions plus one private extension for authority information access, for e.g. validation service)**
  - **CRL (X.509v2 standard fields, and standard extensions)**
  - **Certificate path validation process, basic and extending**

D D S

PKIX and Attribute Certificate profile

- **Farrel, S. (Baltimore), Housley, R. (Spyrus), An Internet Attribute Certificate Profile for Authorization, <draft-ietf-pkix-acx509prof-03.txt>, May 2000**
  defines:
  - **Attribute certificate profile for standard fields and extensions**
  - **Additional attribute types**
  - **Attribute certificate validation**
  - **Revocation**
  - **Usage for authorization**

D D S

PKIX and Qualified Certificate profile

- Santesson, S (Accurata), Polk, W. (NIST), Barzin, P. (Secude), Nystrom, M. (RSA Lab.), Internet X.509 Public Key Infrastructure Qualified Certificates pProfile, <draft-ietf-pkix-qc-03.txt>, February 2000 defines:
  - Qualified Certificate
  - as prescribed by some governmental laws
  - owner is natural person
  - unmistakable identity
  - only non-repudiation as key usage
  - ...

D D S

PKIX LDAPv2 schema

- RFC 2587: Boyen, S. (Entrust), Howes, T. (Netscape), Richard, P. (Xcert), Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999 defines:
  - Objectclass pkiUser with attribute userCertificate
  - Objectclass pkiCA with attributes cACertificate, certificateRevocationList, authorityRevocationList, crossCertificatePair
  - Objectclass cRLDistributionPoint with attributes cn, certificateRevocationList, authorityRevocationList, deltaRevocationList
  - Objectclass deltaCRL with attribute deltaRevocationList

PKIX operational protocols LDAP

- LDAPv2:
  - RFC 2559: Boyen, S. (Entrust), Howes, T. (Netscape), Richard, P. (Xcert), Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2, April 1999. Defines:
  - LDAP repository read
  - LDAP repository search
- LDAPv3:
  - Chadwick, D. (Univ. Of Salford), Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3 <draft-ietf-pkix-ldap-v3-01.txt>. [outdated!] Defines:
  - Which v3 features are needed in PKIX
  - attributeCertificate
  - certificate matching rules

D D S

PKIX operational protocols FTP/HTTP

- **RFC 2585: Housley, R. (Spyrus), Hoffman, P. (IMC), Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP, May 1999**
  - **defines how to FTP and HTTP to obtain certificates from a repository**

D D S

PKIX and certificate validation SCVP

- Malpani, A. (ValiCert), Hoffman, P. (VPN Consortium), Simple Certification Verification Protocol (SCVP), <draft-ietf-pkix-scvp-02.txt>, March 2000
  - Client can offload certificate validation to a dedicated (trusted) server (validity of certificate and certification path)

D D S

PKIX and certificate validation OSCP

- RFC 2560: Myers, M. (VeriSign), Ankney, R. (CertCo), et. Al., X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 1999
  - determination of current status of a certificate without the use of CRLs
  - question contains cert id and time
  - answer contains: “revoked”, “notRevoked” or “unknown”
- Mallam-Baker, P. (VeriSign), OCSP Extension, <draft-ietf-pkix-ocspx-00.txt>, September 1999
  - allows client to delegate processing of certificate acceptance functions to a trusted server

D D S

LDAP work on X.509: Data model

- **Greenblatt, B., LDAP Object Class for Holding Certificate Information, <draft-greenblatt-ldap-certinfo-schema-02.txt>, February 2000**
  - **Introduces Objectclass certificateType**
  - **enables client to retrieve only those certificates that it really wants**
  - **contains attributes: typeName, serialNumber, issuer, validityNotBefore, validityNotAfter, subject, subjectPublicKeyInfo, certificateExtension, otherInfo**

D D S

LDAP work on X.509: TLS Extensions

- **Hodges, J. (Oblix), Morgan, RL (Univ. Of Washington), Wahl, M. (Innosoft), LDAP (v3) Extension for Transport Layer Security, <draft-ietf-ldapext-ldapv3-tls-06.txt>, February 2000**
  - **Extended request/response for Start TLS operation**

D D S

LDAP work on X.509: TLS Usage

- Wahl, M. (Innosoft), Alvestrand, H. (MaXware), Hodges, J., Morgan, RL. (Stanford Univ.), Authentication Methods for LDAP, <draft-ietf-ldapext-authmeth-04.txt>, June 1999
  - Includes (as SHOULD) certificate-based authentication with TLS
  - Client uses Start TLS operation
  - Server requests client certificate
  - Client sends certificate and performs a private key based encryption
  - Client and server negotiate ciphersuite with encryption algorithm
  - Server checks validity of certificate and its CA
  - Client binds with SASL “EXTERNAL” mechanism

D D S

PGP key server

- First only replication of pubring via email
- Marc Horrowitz Keyserver (PKSD)
  - Started 1995
  - Own database backend
  - Email and HTTP interface
  - Operational model (add, revoke, etc.)
  - Net of server
  - Every server has all keys
  - Server synchronisation via email

D D S

PKSD Statistics

- 20 synchronising server
- Almost 1 million keys
- 1,05 GB pubring
- Much more DSS/SH keys than RSA keys
- Most keys only selfsigned (=islands of trust)

D D S

PKSD Problems

- No distributed system
- Permanent server synchronisation causes high bandwith usage
- Chaos when one server is down (bouncing emails)
- No guarantee that a key is replicated on all server
- Not scalable

D D S

New concepts for PGP key server

- PKSD with enhanced backend (Open Keyserver from Highware)
- Keyserver based on DNSSec (www.ietf.org/html-charter/dnssec-charter.html)
- Synchronisation via multicast (G. Baumer, Distributed Server for PGP Keys synchronised by multicast, www.vis.ethz.ch/~baumi/sa/thesis/thesis.html)
- Keyserver based on LDAP (PGP Certificate Server from NAI)

D D S

LDAP PGP-Keyserver requirements

- Standardizes solution
  - data model
  - operational model
- Keys searchable by different criteria
- Certification path followable
- Key status retrievable

D D S

Process of standardization

- 1994 Draft from Roland Hedberg
- 1994 proprietary solution in Tübingen
- Both models fail to include more than one certificate in a person's entry
- 1998 new initiative by DANTE
- DDS and University of Stuttgart take part in the discussion and announce an Internet Draft
- Roadmap: Draft in Summer 2000

D D S

Status of LDAP PGP key server

- PGP test server based on LDAP
- Policy for a service
- Definition of a data model for PGP
- Definition of a format for CAs to send certificates
- Software for storing and retrieving certificates
- A user can store his key into the server via WWW formular

- Model should be enhanced to be sort of PKIX compliant

D D S

Discussion

- A CA based PKI for European NRNs
- Certificate validation
- Certificate path validation
- Where will PCA be?
- Eurocert Project
- ICE-CAR Project