

Certificate implementation— The good, the bad, and the ugly



DOE Security Training Workshop

James A. Rome

Oak Ridge National Laboratory

April 29, 1998

A wealth of riches?



I decided to use certificates for strong authentication, but which ones?

⌘ Entrust

⌘ Entrust WebCA

⌘ Netscape

⌘ SSLeay

⌘ Microsoft IIS

Issues are:

Cost, compatibility, ease of use, flexibility, security

Issues to consider



- ⌘ Do the CA's issue the certificates or do the customers apply for them?
- ⌘ What is the role of a directory server? Is it integrated into the CA? Is it needed?
- ⌘ Can certificates (easily) be used for non-Web applications?
- ⌘ Can the DN contain the information you need?
- ⌘ Will the certificates work in MS & Netscape browsers? Apache, Netscape, MS, ... servers?

Generated-secret method

- ⌘ You know who all your users are.
- ⌘ CA creates a certificate request file ("bulk add file") containing the names and certificate types of the users.
- ⌘ The CA software returns a list of reference numbers and authorization codes (or other means). These "generated secrets" uniquely identify each user.
- ⌘ You must distribute them securely to each user. Each user then visits the Client Interface and enters this information to retrieve the certificate. This generates the keys.

Existing-secret method

- ⌘ Use if the CA doesn't know the names and locations of the people who need certificates, or you don't have a secure way of transmitting reference number and authorization code.
- ⌘ Users generate key pair *before* the request and put the public key in the certificate request.
- ⌘ Must verify the user's identity. In some cases this can be done using an "existing secret" such as a PIN.
- ⌘ Certificate is only useful for private key holder.

Certificate server comparison

	Entrust	WebCA	Netscape	SSLey
\$/Cert	\$140 \$33/year	\$1	free, \$121 \$5+\$10+25	free
Ease of customization	Done in LDAP	Configura- tion file	Easy	Doable
CA Queryable?	No	with difficulty	yes	No
SDK?	Yes (\$5k)	No	Yes (free)	It is one
Initiation	CA	User/CA	User	CA
LDAP integration	Yes	Built-in, queries=?	Manual	No

Prices are hard to figure lately . . .

Product	Base Offering (Includes Media and License)		Price for 10 Additional Users License-Only Pack
	\$ Price	No. of User Licenses	
SuiteSpot Standard Edition	\$5600	50	\$600
Calendar Server	\$1750	50	\$350
Collabra Server	\$525	50	\$100
Directory Server	\$995	100	\$100
Enterprise Pro Server	\$1995	50 (Netshare users)	not applicable
Enterprise Server	\$1295	50 (Netshare users)	\$250 (10 Netshare users)
Messaging Server	\$1295	50	\$250
SuiteSpot Professional Edition	\$7000	50	\$1,025
Certificate Server	\$525	100	\$50
Compass Server	\$1295	50	\$250
Mission Control Desktop	\$995	50	\$200
Proxy Server	\$525	100	\$50
FastTrack Server	\$295	not applicable	not applicable

And there is lots of gamesmanship

NETSCAPE SUITESPOT VERSUS MICROSOFT EXCHANGE AND BACKOFFICE

Price per User Comparison of Shrink-Wrap Product Offerings*

Product	50 Users	100 Users	250 Users	500 Users	1000 Users
BackOffice with SQL Server Internet Connector	329.48	263.93	233.06	230.94	230.94
BackOffice	269.50	233.94	221.06	218.95	218.95
BackOffice Small Business Server with SQL Server Internet Connector	140.06	100.93	77.45		
Exchange Enterprise Edition with SQL Server and SQL Server Internet Connector	303.46	244.25	201.41	210.66	214.38
Exchange Standard Edition with SQL Server and SQL Server Internet Connector	275.44	230.24	195.81	202.76	205.33
SuiteSpot Professional Edition	140.00	121.24	109.98	106.23	104.36
Exchange Enterprise Edition**	101.34	81.03	66.23	69.26	70.46
SuiteSpot Standard Edition	82.00	71.00	64.40	62.20	61.10
Exchange Standard Edition**	73.32	67.02	60.62	61.36	61.40

Browsers and certificates (1)

- ⌘ How do they handle multiple certificates?
 - ◆ 1 certificate/e-mail address.
- ⌘ Can you use a certificate of a person for an alternative e-mail address? (I.e., to send secure e-mail to me if I am at a different location)
 - ◆ No
- ⌘ What does it mean when the browser says a certificate is verified?
 - ◆ It has not expired and it was signed by the CA whose certificate you accepted.

Browsers and certificates (2)

- ⌘ Can certificates be exported from Netscape and imported into IE? It is broken.
 - ◆ Best to download a fresh IE 4.01, install the 128-bit extensions, and then edit the registry.
 - ◆ Use the program regedit. Find HKey_Local_Machine/Software/Microsoft/Cryptography/Defaults/Provider Types and change the value of "Name" string on the TYPE 001 provider from:
Microsoft Base Cryptographic Provider v1.0 to
Microsoft Enhanced Cryptographic Provider v1.0
- ⌘ Both browsers must be 128-bit.

Browsers and certificates (3)

⌘ Can IE 4.01 accept your CA certificate?

- ◆ <http://help.netscape.com/kb/server/970217-8.html>

⌘ Can certificates be spoofed? — Yes

- ◆ NS accepts every certificate in signed E-mail and overwrites existing certificate entry.
 - I issue a certificate to myself in Joe's name
 - I use it to sign an e-mail message to you, spoofing Joe's e-mail address.
 - Your Netscape now has my certificate instead of Joe's.

Netscape certificate download specification at

<http://home.netscape.com/eng/security/comm4-cert-download.html>

What makes a “good” CA?

(Stolen from Stephen Kent, BBN Technologies)

⌘ Primary requirement:

Accurate binding of attributes to a public key.

⌘ Attribute types: identity, authorization, management.

⌘ Is the CA authoritative for its name space, or is this a matter of trust?

- ◆ The smaller the name space, the easier it is to be authoritative.

- ◆ The vision of a global namespace never happened.

Types of CAs

- ⌘ Organizationally empowered
 - ◆ What's good for DOE is good for you.
- ⌘ Geopolitically empowered
 - ◆ I'm from the government and I'm here to certify you.
- ⌘ Universally empowered
 - ◆ Alexander Hague approach.
- ⌘ Liability empowered (third party)
 - ◆ Trust me, I'm a lawyer.
- ⌘ Proprietary
 - ◆ Its my name space, I'll certify what I wish.

Trusted vs authorized CAs

Trust is an elusive issue and hard to quantify.

⌘ No CAs are universally trusted or universally authorized.

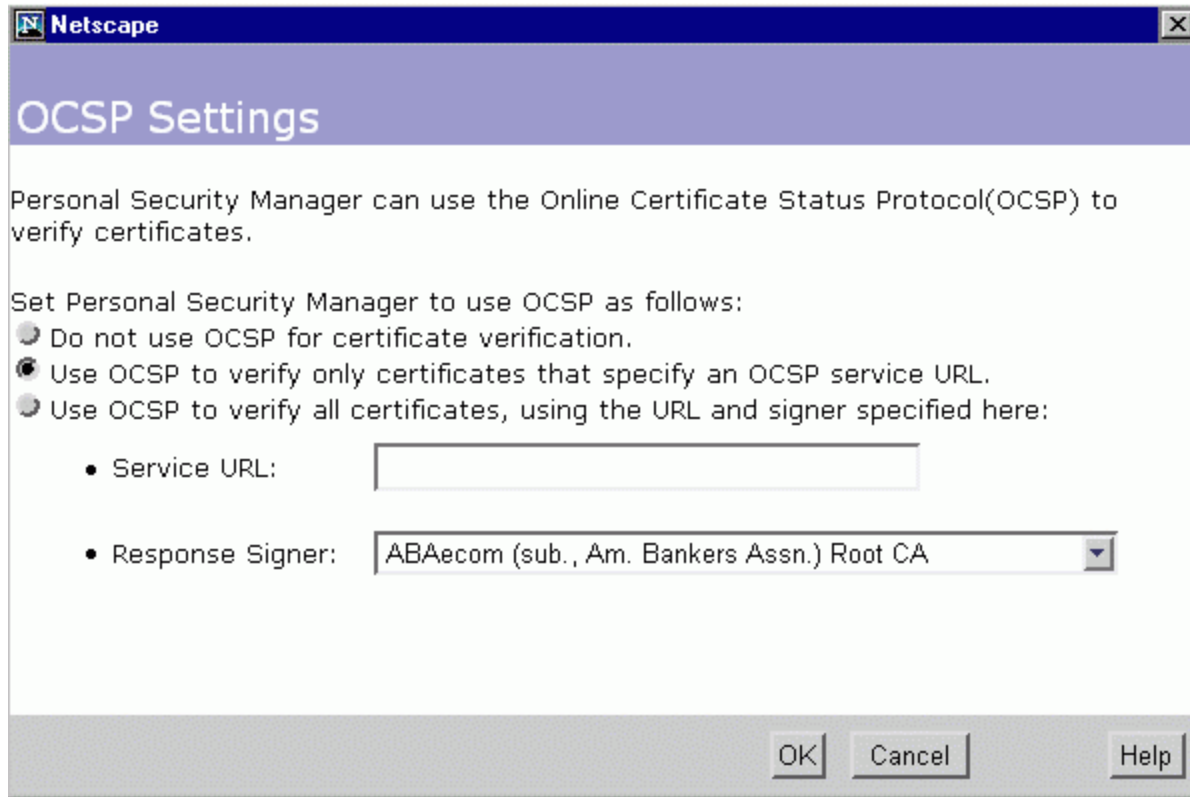
⌘ Authorized CAs:

- ◆ Organizations (employees, clients, members,...)
- ◆ Government (citizens, residents,...)

⌘ Trusted CAs:

- ◆ Third parties (anyone who pays)

Online Certificate Status Protocol



OCSP makes it possible for the Netscape 6 Personal Security Manager to perform an online check of a certificate's validity each time the certificate is viewed or used.

Certificate trust issues



Cross certification is

- ⌘ Complicated

- ⌘ Prone to error

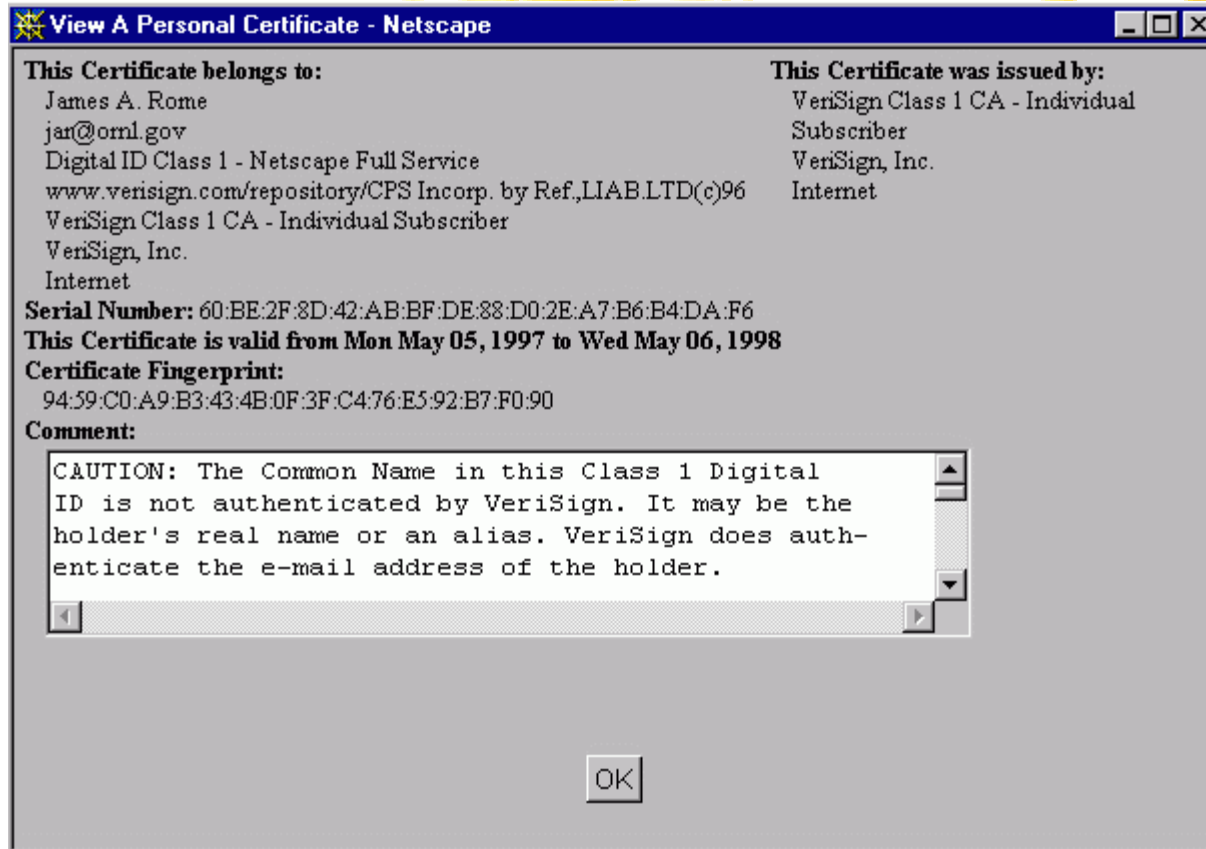
- ⌘ Subject to any “weak link” in the chain

and leaves everyone uncertain of exactly what “certification” means.

CA policy statements

- ⌘ Use as input to access control mechanisms.
- ⌘ Used to specify
 - ◆ security characteristics of the certification process
 - ◆ the revocation procedures
 - ◆ security for user keying material
 - ◆ user authorization information?
- ⌘ Binding policy into certificates
 - ◆ simple identifiers
 - ◆ machine-parsable syntax
 - ◆ pointer to policy statement

CA policy statements



From the VeriSign policy statement

You (the user) acknowledge that (i) **you have been advised to receive proper training** in the use of public key techniques prior to applying for a certificate and that (ii) documentation, training, and education about digital signatures, certificates, PKI, and the PCS are available from VeriSign [§ 1.6].

If you are the recipient of a digital signature or certificate, **you are responsible for deciding whether to rely on it**. Before doing so, VeriSign recommends that you check the VeriSign repository to confirm that the certificate is valid and not revoked, or suspended and then use the certificate to verify [§ 8.1] that the digital signature was created during the operational period of the certificate by the private key corresponding to the public key listed in the certificate, and that the message associated with the digital signature has not been altered.

(vi) the subscriber is an end-user subscriber and not an IA, and **will not use the private key** corresponding to any public key listed in the certificate **for purposes of signing any certificate** (or any other format of certified public key) or CRL, as an IA or otherwise, unless expressly agreed in writing between subscriber and the IA.

VeriSign certificate verification

Search by Email Address (Recommended!)

Enter the email
address:

example: john_doe@verisign.com

Search for IDs that
are:

Valid Revoked Expired Pending All

James Rome (Valid)

jar@ornl.gov

Digital ID Class 1 - Client WebPass ID

Validity period from Nov-15-1997(GMT) to Nov-13-2007(GMT)

James Rome (Expired)

jar@ornl.gov

Digital ID Class 1 - Client Authentication Standard

Validity period from Aug-05-1997(GMT) to Feb-04-1998(GMT)

James A. Rome (Valid)

jar@ornl.gov

Digital ID Class 1 - Client Authentication Full Service

Validity period from May-06-1997(GMT) to May-06-1998(GMT)

Certificates and privacy (1)

- ⌘ I renewed my VeriSign Class 1 certificate and found an (optional) request for my birth date and zip code to embed them in my certificate.
- ⌘ Class 2 certificates also require your address, social security number, driver's license number, spouse's first name.

Certificates and privacy (2)



Can you prevent your certificate from being presented to a site?

⌘ No!!!!

⌘ Once the pass phrase box is presented to you, your only choice is to exit from Netscape (with Task Manager).

⌘ If you dismiss it, it comes back and says that too many incorrect passwords invalidate your certificate database.

CA use issues (1)

- ⌘ No obvious “accept CA” mechanism
 - ◆ A user or site certificate is invalid if the CA that signed it is not on your “approved” list of CAs.
 - ◆ But, no info in the presented certificate on how to get its CA certificate.
- ⌘ In IE it is very difficult to import a Netscape CA root certificate (see previous URL).
- ⌘ In IE 3, it was impossible to form an https SSL session because the site certificate’s CA was not accepted. Hence impossible to get to the CA.

CA unknown failure

These are certificates from other people

allendb1@ornl.gov
elgamal@netscape.com
jimgeuin@cyberservices.com
lpz@ornl.gov
lspitz@newlogic.com
mgmlyna@iname.com
wej@george.lbl.gov
wejohnston@lbl.gov
wrightmc@ornl.gov
yannig@fiu.edu

To get certificates from a network Directory

Search Directory

View A Personal Certificate - Netscape

This Certificate belongs to:

William E. Johnston
wej@george.lbl.gov
ICSD
Lawrence Berkeley National Laboratory
US

This Certificate was issued by:

IDCG-CA
ICSD
Lawrence Berkeley National Laboratory
US

Serial Number: 2E

This Certificate is valid from Fri Feb 06, 1998 **to** Sat Jul 31, 1999

Certificate Fingerprint:

46:93:D1:F6:4B:C1:F5:68:02:EA:AF:A3:E8:D7:F2:77

Verify A Certificate - Netscape

Verification of the selected certificate failed for the following reasons:

wej@george.lbl.gov

Unable to find Certificate Authority

CA use (3)

- ⌘ In Outlook Express, your certificates must exactly match your e-mail address or they will not appear.
 - ◆ How can you handle mail for your ISP and your Lab?
- ⌘ My IE 4.01 crashes Win95 when trying to import the CA certificate. (Worked on NT 4.0.)
- ⌘ Self-signed certificate CAs are subject to attack by imposters.

CA use issues (3)

⌘ Was the certificate revoked?

- ◆ Most certificates do not contain CRL URL.

⌘ Can you get your CA certificate signed by a “higher authority?”

- ◆ No mechanism for this in the Netscape CA.
- ◆ The Lab’s VeriSign certificate cannot be used to sign CA certificates.
- ◆ So, all CA certificates you issue are self-signed.

⌘ Can you query the CA to get information about a certificate?

Distinguished names

The Distinguished name (DN) should pin down the user's "identity," at least within your name space.

⌘ CN=Common Name: *Joe User*

⌘ C=Country: *US*

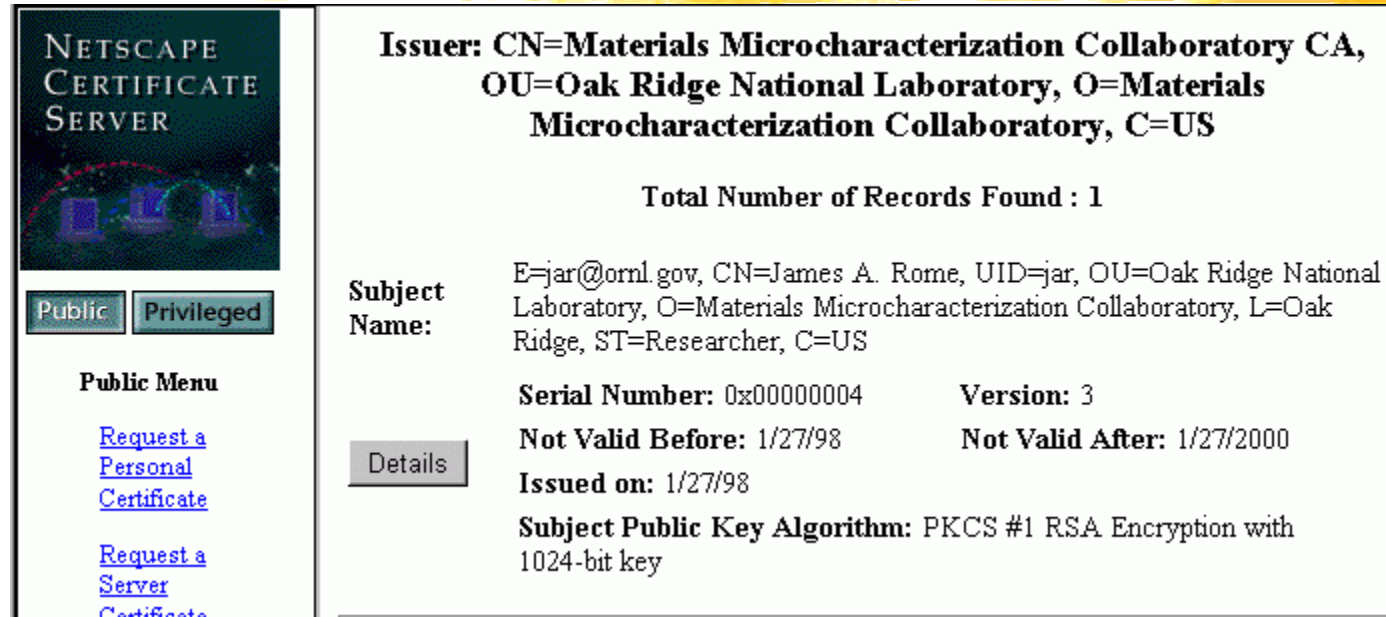
⌘ O=Organization: *Oak Ridge National Laboratory*

⌘ OU=Organizational Unit: *Fusion Energy Division*

Optional fields: ST=State, L=Locality, E=e-mail

The order of the fields matters for the LDAP server.

My certificate (CA query)



**NETSCAPE
CERTIFICATE
SERVER**

Public Privileged

Public Menu

- [Request a Personal Certificate](#)
- [Request a Server Certificate](#)

Issuer: CN=Materials Microcharacterization Collaboratory CA, OU=Oak Ridge National Laboratory, O=Materials Microcharacterization Collaboratory, C=US

Total Number of Records Found : 1

Subject Name: E=jar@ornl.gov, CN=James A. Rome, UID=jar, OU=Oak Ridge National Laboratory, O=Materials Microcharacterization Collaboratory, L=Oak Ridge, ST=Researcher, C=US

Serial Number: 0x00000004 **Version:** 3

Not Valid Before: 1/27/98 **Not Valid After:** 1/27/2000

Issued on: 1/27/98

Subject Public Key Algorithm: PKCS #1 RSA Encryption with 1024-bit key

Details

Note: The MMC has overloaded the State (ST) field to mean "status." This serves as part of a role-based access control mechanism (RBAC).

CA query

Bookmarks Netsite: <https://mmc.epm.ornl.gov:4433/index-netscape.html>

Certificates Pubs Meeting Sites FileRoom Web CIS Security Kerberos NT My Stuff LM MMC Lookup

NETSCAPE CERTIFICATE SERVER

Public Privileged

Public Menu

- [Request a Personal Certificate](#)
- [Request a Server Certificate](#)
- [Search for Certificates](#)
- [List Certificates](#)
- [Accept This Authority in Your Navigator](#)
- [Accept This Authority in Your Server](#)
- [Review Certificate Revocation List](#)

Notify [Jim Rome](#) of your request

Search For Certificates

This form allows you to [search for certificates](#) by the owner's name.

Enter values for those fields that you wish to have in your search criteria. Leave other fields blank.

E-mail Address:

Common Name:

User ID:

Organization Unit:

Organization:

Locality:

Status:

Country:

Match Method

Exact Find certificates for subjects whose name consists *exactly* of the components that you have filled in above, and contains none of the components you have left blank. Pattern matching wildcard values cannot be used in this search.

Partial Find certificates for subjects whose name consists *in part* of the components you have specified above, and in addition may contain arbitrary values for the other components you have left blank above. Pattern matching wildcard values can be used in this search.

Do not show certificates that have been [revoked](#)

Do not show certificates that have expired or are not yet valid

Document: Done

Better way to name the CA

Instead of “MMC CA,” use

“https://mmc.epm.ornl.gov:4433” as the CA name.

⌘ Then, the user who sees the unknown CA can access the site and decide whether to accept its certificate.

⌘ He can also check that the site is really at ornl.gov and read a blurb about the MMC.

Including the CA URL is a proposed extension to X.509.

How secure is your CA?

- ⌘ If the CA private key is compromised, so are all certificates issued by that CA.
- ⌘ The degree of security should be commensurate with the risk involved.
 - ◆ Money = high risk
 - ◆ Collaboratory = lower risk
 - ◆ SET private key is in about a dozen hardware tokens scattered throughout the world. Only a quorum is needed to conduct business.
- ⌘ High-security CAs use hardware key generation and CMW (B1 security level) platforms.

Web servers and certificates

- ⌘ By default what does a server do with a client certificate? Is it checked for
 - ◆ validity?
 - ◆ revocation? (Even VeriSign has no CRL)
 - ◆ the CA validity?
 - ◆ anything??
- ⌘ The certificate does not contain information about the certificate server or the LDAP server that stores the associated user information. So, where do you access them?

Client authentication process

- ⌘ A client (such as a browser) requests a connection with the server.
- ⌘ The server is authenticated or not (through the process of server authentication).
- ⌘ The client signs but does not encrypt its certificate and sends it to the server.
- ⌘ The server uses the client's public key, which is included in the certificate, to verify that the owner of the certificate is the same one who signed it.

Client authentication (cont.)

- ⌘ The server attempts to match the certificate authority to a trusted certificate authority. If the client's certificate is not listed as trusted, the transaction ends, and the client receives: "The server cannot verify your certificate."
 - ◆ If you want to restrict access to users with your certificates only, just eliminate all CAs except your own from the server's list of trusted CAs.
- ⌘ If the client's certificate authority is trusted, some servers fulfill the transaction. (!!)

Client authentication (cont.)

- ⌘ Next, the server needs to match the information from the certificate with an entry in an LDAP directory (why??) to further identify and authenticate the user. If all information matches, the server accepts the client as authenticated.
- ⌘ If entries in your database contain certificates rather than information, the server compares the sent certificate to the one in the database. If they match, the server grants the client access.

How to use DN without LDAP

Netscape says:

“Use the Access-Control API to implement your own attribute getter function for the user attribute when the authentication method is SSL. Your attribute getter function can extract the issuer and subject DN's from the user certificate and construct SQL queries to the third-party database.”

Microsoft says:

“It is all in the platform development kit”

Its easier said than done....

References

DOE ER/DP Security Research Needs Workshop (PKI)

- ◆ <http://www-itg.lbl.gov/security/workshop/>

Introducing SSL and Certificates using SSLeay

- ◆ <http://www.camb.opengroup.org/RI/www/prism/wwwj/index.html>

NIST PKI program

- ◆ <http://csrc.ncsl.nist.gov/pki/welcome.htm>

Overview of Certification Systems: X.509, CA, PGP and SKIP

- ◆ <http://www.mcg.org.br/cert.htm>

Akenti authorization certificates (LBNL — William Johnston)

- ◆ <http://www-itg.lbl.gov/security/Akenti/>

Carl Ellison on SPKI authorization certificates

- ◆ <http://www.clark.net/pub/cme/html/spki.html>