

PKI in the Small

A Public Key Infrastructure for
Advanced Network Technologies Workshop
April 27–28, 2000, NIST

James A. Rome

Executive Secretary, IST

Center for Information Infrastructure Technology

DOE Y12, Advanced Technology Directorate

Oak Ridge, Tennessee 37830-8027

(865) 574-1306 jar@y12.doe.gov

<http://www.ornl.gov/~jar>





Some uses of PKI

- Authentication of people, resources, places
- Encrypt and/or digitally sign
 - ◆ E-mail
 - ◆ Code objects
 - ◆ Communication channels
- Basis for strong authorization
- Keystone of secure applications

What issues arise when you actually want to use PKI in an application-based infrastructure?



What does an X.509 certified @

PKI X.509 certificates bind an identity to a public key

The person with the distinguished name

E=jar@y12.doe.gov, CN=James A. Rome, UID=jar, L=Oak Ridge\, TN, ST=Administrator,
OU=Center for Information Infrastructure Technology, O=Materials Microcharacterization
Collaboratory, C=US

is known by the public key

30:81:89:02:81:81:00:B1:F1:FC:D0:D8:6F:B3:71:73:
36:6B:5F:1C:9F:9B:5B:E9:35:84:95:A1:C0:2D:B2:E5:
5D:0F:8C:B8:4E:78:69:B8:BB:E3:71:B5:C2:AB:08:8A:
8F:47:3C:51:CB:AC:F2:F3:D0:B4:2F:2F:34:F7:E1:1D:
30:D5:51:F1:72:F9:3D:AE:C1:5D:5B:26:39:5A:DA:10:
CF:A3:3E:95:99:7A:F3:27:79:88:7A:BC:E4:9A:F6:39:
87:9A:49:E0:70:9A:E4:B4:29:93:33:C0:41:59:FB:41:
B6:D8:B1:A7:39:FC:5D:17:1B:75:AF:B2:81:EC:EE:E7:
A7:A7:FB:85:17:B1:33:02:03:01:00:01



Is this enough?

- There is at least one more *James A. Rome*
(I own his paintings!)
- Is the information in the DN enough to pin down which *James A. Rome* you want to deal with in a large trust realm? How about *John Smith*?
- Do you accept the assurances of the authority that issued my certificate?
(Issuer: CN=MMC CA,OU=Center for Information Infrastructure Technology,O=Materials Microcharacterization Collaboratory,L=Oak Ridge\,TN,ST=Administrator,C=US)
- Is my certificate valid right now?
- Do you want to trust me for everything?



It suffices in some situations

A bank, the IRS (One-way trust)

- They only care that you identified yourself with a valid social security number (your “identity”)
- As long as there is money in the account the PKI certificate from a bank identifies its customer for its purposes
 - ◆ If you are a crook, it is someone else’s problem
- Your social security number is a unique government identifier, but you may have many certificates
 - ◆ What information do you want in your certificate?
 - ◆ What information does the issuer want in it?
 - ◆ What ever happened to privacy?

Certificates may only be a first step in others...



The whole Canadian government has Entrust certificates

- Can you use the certificates to really identify the person you want?
- Should they be trusted? (Two-way trust)

In general, an out-of-band method is needed to really identify someone to your satisfaction

- You know someone who knows him (PGP)
- You met them at a meeting and have their e-mail
- The owner of a resource says “OK”



Size of the trust realm matters

- A collaborative works well
 - ◆ ~100 people
 - ◆ PGP model of trust works
 - ◆ Members unlikely to become criminals overnight
- A National Laboratory is kind of big
 - ◆ Everyone has a government badge, including
 - grad students from India
 - janitors, guards, secretaries, scientists
 - ◆ Can you tell which is which?
 - ◆ For some things it matters

The applications using PKI must enforce restrictions



Authorization is what counts

PKI can provide strong authentication, but only the owners of resources can authorize their use

- How do you use certificates in the authorization process?
- Can you guarantee that stakeholder rights are enforced? (See Akenti in my other talk)
- Is there an audit trail for legal action in case of criminal activity?
- Who determines and maintains the security policies?



Security and Networking

With million-\$ instruments on line, security is a necessity.

- Fast, transparent encryption
- Secure multicast for conferencing and group collaboration
- Accurate and fast knowledge of who is accessing our devices from across the net

Certificates are the key to achieving above



So you want to set up PKI?

A PKI infrastructure is the most mature solution available for implementing security

- SSL-based Web servers
- SSL hooks in Java, CORBA, Entrust toolkits
- Client certificate management in Netscape and IE
- S/MIME e-mail
- Signed Java and JavaScript applets
(override security of sandbox)
- Server-side programs
- Stand-alone applications

So, what is involved in deploying these tools?



Which certificates to use?

Certificates issued by agency or Laboratory:

- Users may already have certificates to support other applications
- Organization accepts cost of maintaining infrastructure
- Probably will be part of FPKI
- Certificates are fairly generic

Certificates issued by collaboratory or project:

- Local control over certificate content
- Easier to identify authorized users
- May not be recognized by FPKI



SSL Web servers

Netscape, IIS, and Apache (Stronghold) all support SSL encrypted channels.

- It is easy to configure a Web server to require certificates and to only accept those from one CA
- You need a server certificate
 - ◆ Minimum cost is ~\$300
 - ◆ You may need a Dunn and Bradstreet report and letter from the company President,...
- ORNL uses Thawte server certificates
- You probably want to issue your own server certificates . . .



Certificate Authorities (CAs)

Certificate Authority software allows you to issue server and client PKI certificates

- Roll your own with SSLeahy or newer toolkits
 - ◆ Bad idea. No tools, no user interfaces, etc.
- Buy one from Netscape, Entrust, ...
 - ◆ Netscape cost ~\$31 (internal), \$8 (external) per certificate
- You want your CA to be on a secure machine (locked room, not a lot of other things on it).
- What should the Federal policy on recognizing these CAs be?



Client certificates stored in browsers

- Hard to use on someone else's computer (you cannot put the certificate on a floppy disk and use it directly)
- Only the latest browsers can manage certificates

Select Your Certificate:

Joe Nato's Materials Microcharacterization Collaboratory ID
 Joe Nato's Materials Microcharacterization Collaboratory ID
 James Rome's Materials Microcharacterization Collaboratory ID
 James A. Rome's Materials Microcharacterization Collaboratory ID
 MMC CMS Administrator's Materials Microcharacterization Collaboratory ID
 James A. Rome's VeriSign, Inc. ID #2 (expired)

Client Authentication



The Web site you want to view requests identification. Select the certificate to use when connecting.

James A. Rome
 James A. Rome
 James A. Rome

- It is very difficult to create Web applications that can access the client certificate DN directly, so that you can use it to implement policy decisions
 - ◆ The usual APIs expect access via LDAP servers
- It is almost impossible to allow a user to access his private key outside of the browser



Browser sand certificates

- How do they handle multiple certificates?
 - ◆ 1 certificate/e-mail address.
- Must use Netscape or IE5. IE4 never worked properly.
- Can certificates be spoofed? — Yes
 - ◆ NS accepts every certificate in signed E-mail and overwrites existing certificate entry.
 - ◆ Only stores user certificates by e-mail address.





CA issues

- No obvious “accept CA” mechanism
 - ◆ Certificate is invalid if the CA not on your “approved” list. But no info on how to get the CA certificate.
- Most certificates do not contain CRL URL
- Generally no ip address for the CA or LDAP server in the presented certificate
- What does “certificate is valid” mean?
 - ◆ CA on approved list
 - ◆ Today is in the certificate validity range
 - ◆ Netscape 6 will allow you to designate a place to verify certificates (all or nothing)



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

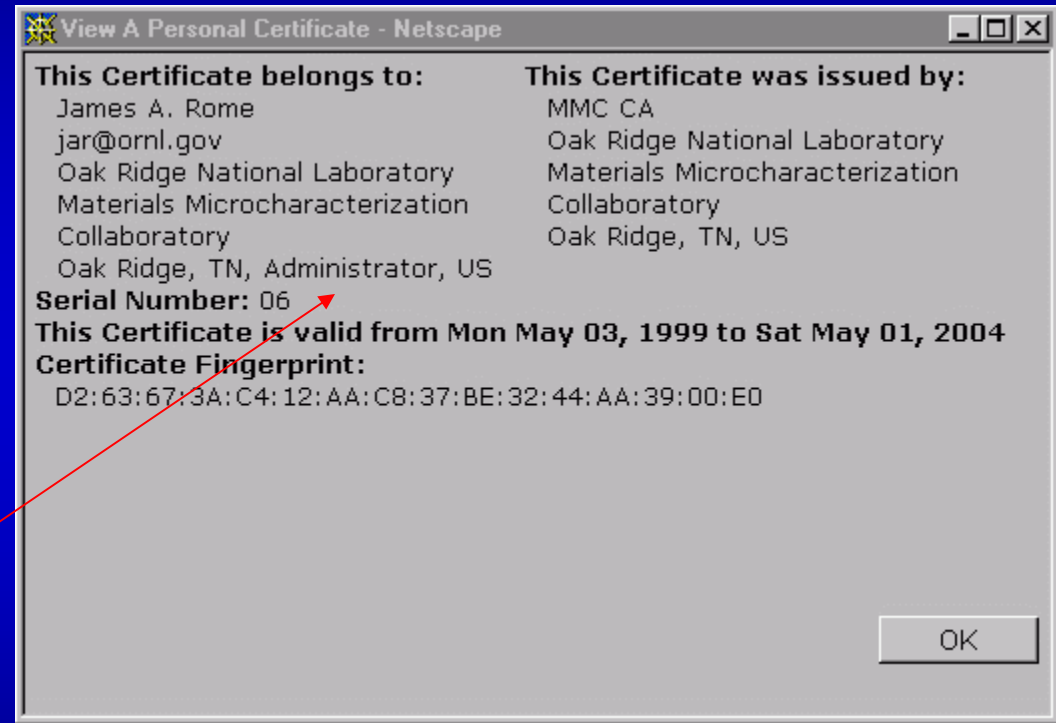
Unable to find Certificate Authority



Role based access may suffice

Broad user categories might suffice to define access permissions.

This role can be embedded in the user's certificate if you have control over what goes into your certificates.





Summary

Getting PKI certificates is only a small part of the process. Many issues must be resolved:

- Which certificates and CA will you use?
- What sort of PKI-enabled applications will you support?
- How will the “out-of-band” information about the certificate holder be obtained?

If it is not made easy and advantageous for the user, it will not be used