PKI & identity

Technical and legal aspects

Hoyt L Kesterson II
Editor for X.509 | 9594-8
26 September 2007

Is this the party to whom I'm speaking

- Every entity should have a name
- It's OK to have more than one name
- But no two entities should have the same name
- *I am me* may work in my domain
- But it fails when I want to talk to the world

The Distinguished Name

- X.500 Directory specifies the Distinguished Name
  - Hierarchical and typed
  - Country=Freedonia, Organization="Defense Department", Common Name=Chicolini
- Assumes Registration Authorities will handle naming
  - One isn't qualified to discuss this topic unless one can correctly use *unique* and *unambigious* in the same sentence
- This hasn't gone as smoothly as hoped
  - *Badges? We don't need no stinkin badges*

Proving you're you and I'm me

- The X.509 Public-key certificate securely associates
  - the distinguished name of an entity; and,
  - the public key of that entity
- The entity has a private key that is securely associated with the public key
- There are functions, typically calling signing, that proves that the entity knows the private key
- One trusts the association of the public key and the name because the certificate is signed by a trusted entity, the Certification Authority (CA)
- One trusts the CA because…well, it's turtles all the way up

All these names are me

- Certificate can hold one or more names in different name syntaxes
  - RFC 822 email name
  - DNS name
  - X400 name
  - EDI party name
  - URI, universal resource identifier
  - IP address
  - Registered name, OID
- All the alternate names will be securely associated with one entity

You can add stuff

- X.509 (and the directory protocols also) are extensible
- Anyone can add a new extension to a certificate for a new function
  - ITU and ISO/IEC extends the certificate by adding new extensions
  - The IETF has defined extensions
- Relying parties are required to ignore fields they don't recognize

Unless

that extension is marked critical

The standards work

- ITU Rec. X.509 and ISO/IEC 9594-8 first published in 1988
  - Fifth edition in 2005; sixth edition coming in 2009
  - X.509 specifies public-key certificate and attribute certificate
  - The X.500 series defines the directory and name structure
  - Naming & addressing, and Registration authorities are standardized
    - ISO/IEC 9834 and ITU X.660 series of Recommendations
- The IETF is a significant contributer
  - PKIX implementor profile
  - Additional extensions in the certificate
  - Protocols to distribute, validate, and determine the status
  - LDAP directory

Using a certificate — SSL (PG-13)

1) browser creates random value and sends to server along with supported cipher methods

2) server creates random value and sends it, its public key certificate(s), and selected cipher method to the browser

3) browser validates server's certificate and determines if communicating with correct server

a modern browser

a modern server

Using a certificate — SSL (PG-13)

4) browser generates a random value and encrypts it using the server's public key

5) browser sends that encrypted value to server

6) server uses its private key to decrypt the received value

7) browser and server use that shared secret value and the two publicly exchanged random values to create shared secret values for encryption and integrity

a modern browser

a modern server

Using a certificate — SSL (PG-13)

8) browser sends MAC of messages (1, 2, & 5) to server

9) server sends MAC of messages (1, 2, & 5) to browser

a modern browser

a modern server

Using a certificate — SSL (PG-13)

10) a secure pipe is established

a modern browser

a modern server

I AM NOT A LAWYER

The lawyers are interested

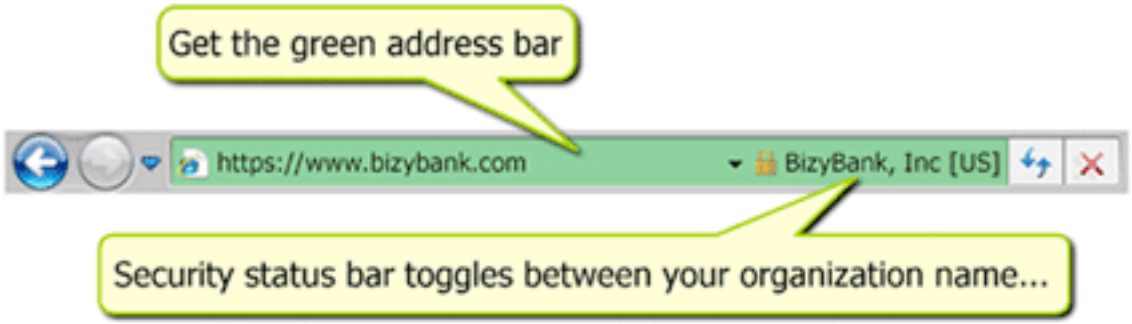
- Lawyers care about identity
- Signing ceremonies authenticate identities
- Dispute resolution typically requires validated information, including authenticated identification of parties
- Lawyers don't like ephemeral or ambiguous names
- They can work with descriptive name forms, the John Smith who is not a horse thief

The lawyers have been doing things

- US, Canadian, and EU legal experts worked with Directory and PKI experts
- In the US the American Bar Association produced the Digital Signature Guidelines and the PKI Assessment Guidelines
- Most countries have passed electronic signature laws and regulations
- ABA recently worked with browser implementors to “fix” the issuing of certificates
  - Browsers downplayed the need to validate the identity of the web site
  - Users clicked through frequent and obscure certificate warnings

Because “they” didn’t get it right the first time

- CAs did not perform *due diligence* checks on names
- Phishing emails lead to spoofed sites and fraud
- For extended validation the CAs will do the work they should have been doing before issuing SSL certificates, e.g. is the organization registered with the Secretary of State’s office
- Browsers will signal the presence of “more trusted” certificates



One of your goals should be to ensure “they” get it right the first time

Thank you. Questions?

Hoyt L. Kesterson II
Independent Consultant
7625 West Villa Rita Drive
Glendale, Arizona 85308
hoytkesterson@earthlink.net
+1 602 316 1985 (ether)
+1 602 978 3298 (copper)