certspec (in brief)

Sean Leonard, Penango, Inc.

IETF 84 PKIX

Wednesday, August 1, 2012

What is certspec?

urn:cert:issuersn:CN=Atlantis;2A

- Uniform syntax for
- identifying
- a *specific* certificate
- in a textual format

URN Primer

- Resource identifiers that are **persistent**, **location-independent**, **text-based** (**transcribable** by keyboard & **recognizable** by humans), **mappable** to other URIs
- RFC 2141; urnbis
- Examples:
  - urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
  - urn:oid:1.3.6.1.4.1
  - urn:ietf:rfc:2141
  - urn:isbn:0-395-36341-1

Motivation

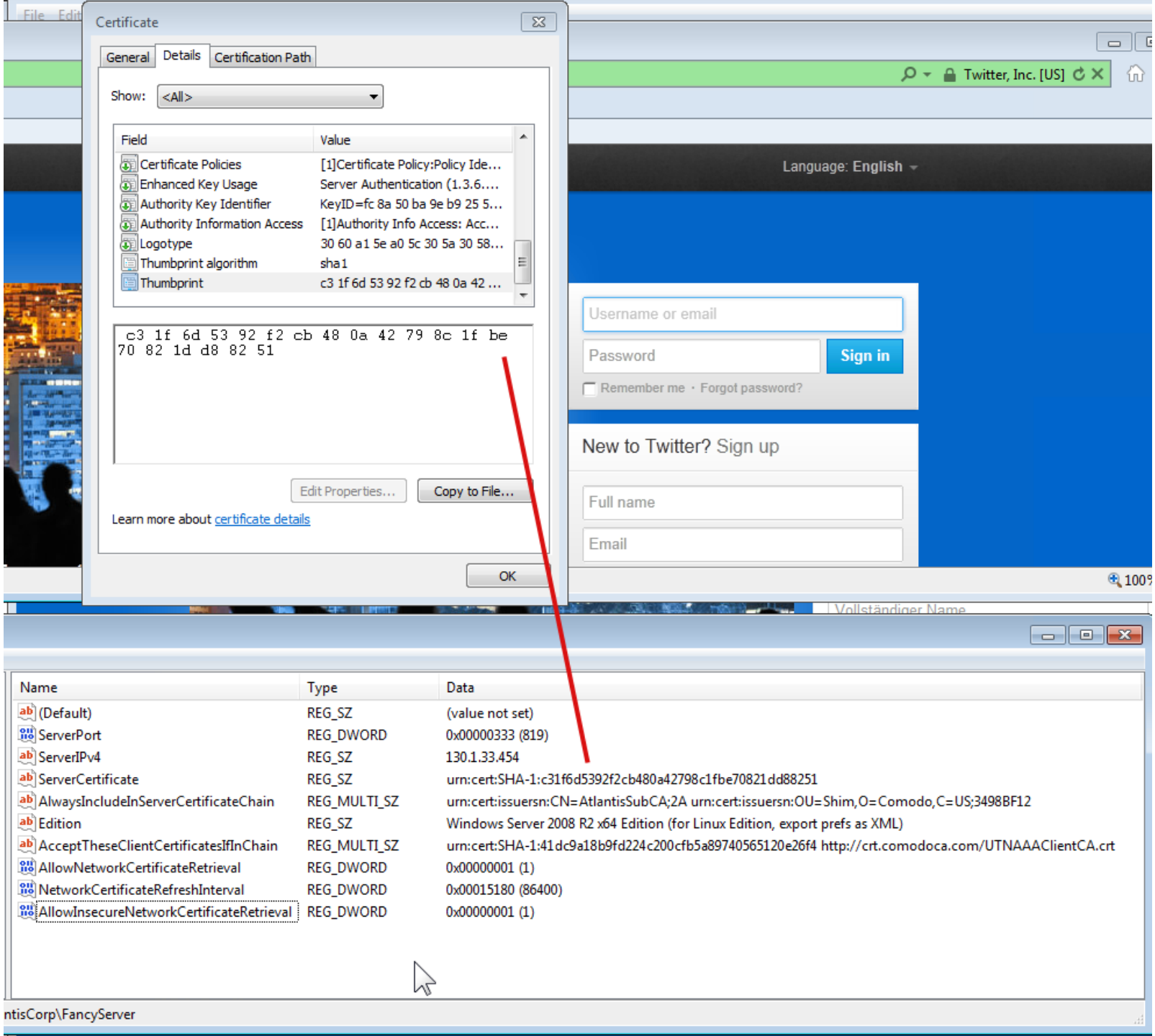
- Apps
  - in preferences for runtime retrieval
  - for exchange
- Protocols

—IN TEXT—

Mechanisms

`urn:cert:SHA-256:0de4564b…fa592f58`

- by-reference
  - by-hash (SHA-1, SHA-2)
    (not “parameterized”)
  - by-data (issuersn)
- by-value
  - data (base64, hex)


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Certificate Policies
[1]Certificate Policy:Policy Ide...
Enhanced Key Usage
Server Authentication (1.3.6....
Authority Key Identifier
KeyID=fc 8a 50 ba 9e b9 25 5...
Authority Information Access
[1]Authority Info Access: Acc...
Logotype
30 60 a1 5e a0 5c 30 5a 30 58...
Thumbprint algorithm
sha1
Thumbprint
c3 1f 6d 53 92 f2 cb 48 0a 42 ...
c3 1f 6d 53 92 f2 cb 48 0a 42 79 8c 1f be
70 82 1d d8 82 51
Edit Properties...
Copy to File...
Learn more about certificate details
OK
Twitter, Inc. [US]
Language: English
Username or email
Password
Sign in
Remember me · Forgot password?
New to Twitter? Sign up
Full name
Email
Name
Type
Data
(Default)
REG_SZ
(value not set)
ServerPort
REG_DWORD
0x00000333 (819)
ServerIPv4
REG_SZ
130.1.33.454
ServerCertificate
REG_SZ
urn:cert:SHA-1:c31f6d5392f2cb480a42798c1fbe70821dd88251
AlwaysIncludeInServerCertificateChain
REG_MULTI_SZ
urn:cert:issuersn:CN=AtlantisSubCA;2A urn:cert:issuersn:OU=Shim,O=Comodo,C=US;3498BF12
Edition
REG_SZ
Windows Server 2008 R2 x64 Edition (for Linux Edition, export prefs as XML)
AcceptTheseClientCertificatesIfInChain
REG_MULTI_SZ
urn:cert:SHA-1:41dc9a18b9fd224c200cfb5a89740565120e26f4 http://crt.comodoca.com/UTNAAAClientCA.crt
AllowNetworkCertificateRetrieval
REG_DWORD
0x00000001 (1)
NetworkCertificateRefreshInterval
REG_DWORD
0x00015180 (86400)
AllowInsecureNetworkCertificateRetrieval
REG_DWORD
0x00000001 (1)
ntisCorp\FancyServer

Compare certspec with others

- Existing preferences not portable, exchangeable, or algorithm-agile
- Different protocols reinvent the wheel
- Want by-value and by-ref agility
  - eliminates DoS vector, lookup time

certspec URN	ni URI
URN for certs	URI for any digital object
Canonical enc / unique ID	No canonicalization / not unique
No truncation allowed (“security”)	Truncation encouraged (“flexibility/brevity”)
copy & paste, visual comparison from existing crypto tools	Full support requires new implementations; base64url support

Next Steps

- (Probably) in Apps WG
- Harmonize with urnbis
- Want to publish something relevant to implementers and users
- Improve Motivation section

Questions?