pkix-textual

Sean Leonard, Penango, Inc.
(with Simon Josefsson, SJD AB)

IETF 84 PKIX

Wednesday, August 1, 2012

pkix-textual

```
-----BEGIN CERTIFICATE-----
MIIDyTCCArGgAwIBAgICD1kwDQYJKoZIhvcNAQELBQAwdTELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExFDASBgNVBAcTC0xvcyBBbmdlbGVzMR8wHQYD
VQQJExYyMDI5IENlbnR1cnkgUGFyayBFYXN0MQ4wDAYDVQQREwU5MDA2NzEKMAgG
A1UEAxMBUTAeFw0xMjA4MDEwNzE0MzhaFw0xNDA4MDEwNzE0MzhaMHUxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRQwEgYDVQQHEwtMb3MgQW5nZWxl
czEfMB0GA1UECRMWMjAyOSBDZW50dXJ5IFBhcmsgRWFzdDEOMAwGA1UEERMFOTAw
NjcxCjAIBgNVBAMTAVEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDj
I9lFFgoFBXBcOlKc6RnpzT2LkbfbKpp4NXLiKB5UAcqlrRVzRYPBusXQ/1VrLTWF
LB0iCK29lyibTKgwcOVp3K21itJezk/WK3c7a6Vo2rSTy5ht46YVcFPUXu7wPU5I
Uz6f7G8WVuiwUgbMMVUM1Aqcl7B4kzxmwgRjjSvc/LYfXWb6uke73q6KmekGEcz9
hdQEGTz93OSwnavdnt5DWUsDbYOctqpjBsC06pvyh/PrYV82awE18DRXutGQYgox
RxuNJjQeSxWF9Q+w6Gofo/Uy8HlrQrsUEUPe82CUMKQAoTO6mQqaO6bWi72n7Oic
sAgZii16N4Ezm9CehWszAgMBAAGjYzBhMB0GA1UdDgQWBBQb7wNzQrXCIv3oYY8e
3EjzveYh/zAMBgNVHRMBAf8EAjAAMDIGCWCGSAGG+EIBDQQlFiNJJ3ZlIEdvdCBh
IExvdmVseSBCdW5jaCBvZiBDb2NvbnV0czANBgkqhkiG9w0BAQsFAAOCAQEAKAeP
aBrfEka2s4DfdiHydt2PGmzOAJ5czTnh/AqHkeYqZacJjK02N5etm/FLRlYDWlca
NkszM2XTs5+BwMN6Up4Hhd8aCFLB49JMfU+ckHDZUu9VokNCgcPQsPldoMe6Xq4m
7mdDp6ZaF8f6zD//RdfEzMD4b5tDocGDNJp+LVFNdY9AQyG5t8DjYoY+5ol8wCkR
LgQ9th0l8XGKAAcF9NVkfNLEIhvkXTX2AeUn5BPZRSDnoq2pN6H9bUl+OYsDAVWc
K30F5qZyO3SkSiLvHIAPQuUdRwGT3KyEJ/zQ1eA5nW/8Pz1HRwRDjofxksRBROgh
gLLERkSLb1g2wpHo8Q==
-----END CERTIFICATE-----
```

- Text encodings of PKIX *and* CMS structures

History

- Privacy Enhanced Mail (RFC 1421)
  - "encapsulated PEM message"
  - ≠ this encoding ("PKIX text encoding?")
- Proliferation and apathy
- Other Variations
  - OpenPGP "ASCII Armor"
  - OpenSSH "Key File Format"

Goals of RFC

- **Document existing practice**
- Go with what is already working
- Avoid new stuff

Extensive Interoperability Testing

- 24 variations of data
- 4 crypto stacks
  - CryptoAPI Windows 7 (6.1 SP1)
  - Mozilla NSS 3.13.5
  - OpenSSL 1.0.1c
  - Apple Keychain 4.1.1 (Mac OS X 10.6.8)
- 3 profiles
  - Strict output
  - Strict input
  - Lenient input

Surprising results!
(unless already jaded)

PKIX Structures Covered

-----BEGIN

Structure	Label
Certificate	CERTIFICATE
CRL	X509 CRL
PKCS #10 Certification Request	CERTIFICATE REQUEST
PKCS #7	PKCS7
CMS	CMS
PKCS #8 (Private Key Info)	Multiple identifiers
PKCS #8 (Encrypted Private Key Info)	ENCRYPTED PRIVATE KEY

Next Steps

- WG Adopt
- More interoperability testing?
- Improve history section?
- Additional structures?

Questions?