Report on Certificate Tools

Oliver Bodnár

August 2016

Contents

Part I

Overview

Chapter 1

Overview Tables

1.1 General

Table 1.1: Overwiew General

Tools	General		
	Type	View and information	License
OpenSSL	PKCS12	Yes	Public
Keygen	JKS		

1.1.1 Type

This section defines type of storage file in which the certificates or keys are saved. Most common are PKCS#12 (.pfx and .p12 extentions) and JKS (Java KeyStore).

1.1.2 View and information

This section shows whether it is possible to view certificates or keys and additional information. Yes means that at least viewing is supported while not necessary meaning possibility of viewing more information about certificate.

1.1.3 License

Type of license and possibility of using said tool for testing or production code. Public means that license is not requiered for use in production code but does not mean that it should be used as such. Definition if it is advised to use said tool in production code or only in testing enviroment will be talked about in the next chapter under each tool.

1.2 Generation and signing of certificates

1.2.1 Keys, certificates and basic constraints

Table 1.2: Generation of keys and certificates and basic constrints

Tool	Generate keys				Basic Constraints	
	+ self-signed certificate	+ CSR	Specify length	Specify algorithm	Specify Type	Specify path length
OpenSSL	Yes	Yes	Yes	Yes	Yes	Yes
Keygen						

Generate keys

Self-signed certificate possibility of using 1 command to generate key pair and self-signed certificate

Certificate Signing Request possibility of using a command to generate key pair and certificate signing request to certificate authority.

Specify length possibility to specify the length of output key

Specify algorithm possibility to choose between different types of algorithms for key generation

Basic Constraints

Specify Type specify if generated certificate will belong to certificate authority or whether it will be end certificate

Specify path length specify the maximum length of certificate authority chain

1.2.2 Specifications

Table 1.3: Specifications

Tool	CSR signing	Privkey + signed chain	Specify certificate validity	SAN for end certificates	Support for CSP
OpenSSL	Yes	Yes	Yes	Yes	Yes
Keygen					

Certificate Signing Request signing possibility of signing a certificate signing request with certificate authority's key

Create combination of private key and signed chain possibility of generating private key and chain signed by certificate authority that will be outputed to a single file

Specify certificate validity possibility of choosing how long will the certificate be valid. This should be done by certificate authority.

Setting Subject Alternative Name for end certificates possibility of choosing Subject Alternative Name for end certificates. That should be done by IP's or DNS addresses.

Support for Cryptographic Service Provider whether the use, choosing and changing of Cryptographic Service Provider is supported.

1.3 Conversions

Table 1.4: Conversions

Tools	Exporting		Direct JKS and PKCS12	Import certificate and private key into a file
	Certificate/chain only from file	Private key only		
OpenSSL	Yes	Yes	No	Yes
Keygen				

1.3.1 Exporting

Certificate or certificate chain from a file

Possibility of extracting certificate or certificate only from a file. Choice of Yes based on possibility of extracting either from a file.

Private key only

Possibility of extracting private key from tool's file storage type of choice.

1.3.2 Direct conversion between Java Keystore and PKCS#12 file

Possibility of direct conversion (by a command of tested tool) between Java KeyStore and PKCS#12 type file.

1.3.3 Importing of certificates and keys into storage files

Possibility of importing (additional?) certificates and keys into storage files of said tool. Yes if it is possible to import or add another certificate or key into storage.

Part II

Tools

Chapter 2

OpenSSL

2.1 General

2.1.1 Type

OpenSSL uses PKCS12 to store keys and or certificates. Certificates and keys made in OpenSSL however are being made into PEM or DER encoded file. Said keys/certificates can then be stored inside single .pfx file.

2.1.2 View and information

Viewing stored certificates

PEM encoded certificates (.pem|.cer|.crt): `openssl x509 -in sample_cert.extention -text -noout`

DER encoded certificates (.der): `openssl x509 -in certificate.der -inform der -text -noout`

Importing PEM or DER encoded keys or certificates into PKCS12 file: `openssl pkcs12 -export -in file.p`
certfile option is used only if importing more certificates into a single PKCS#12 file is wanted.

2.1.3 License

2.2 Generation and signing of certificates

2.2.1 Keys, certificates and basic constraints

Generate keys

Self-signed certificate

Certificate Signing Request

Specify length

Specify algorithm

Basic constraints

Specify Type

Specify path length

2.2.2 Specifications

Certificate Signing Request signing

Create combination of private key and signed chain

Specify certificate validity

Setting Subject Alternative Name for end certificates

Support for Cryptographic Service Provider

2.3 Conversions

2.3.1 Exporting

Certificate or certificate chain from a file

Private key only

2.3.2 Direct conversion between Java Keystore and PKCS#12 file

2.3.3 Importing certificates and keys into storage files

Chapter 3

Keygen

Chapter 4

Tool Page Template

4.1 General

4.1.1 Type

4.1.2 View and information

4.1.3 License

4.2 Generation and signing of certificates

4.2.1 Keys, certificates and basic constraints

Generate keys

Self-signed certificate

Certificate Signing Request

Specify length

Specify algorithm

Basic constraints

Specify Type

Specify path length

4.2.2 Specifications

Certificate Signing Request signing

Create combination of private key and signed chain

Specify certificate validity

Setting Subject Alternative Name for end certificates

Support for Cryptographic Service Provider

4.3 Conversions

4.3.1 Exporting

Certificate or certificate chain from a file

Private key only

4.3.2 Direct conversion between Java Keystore and PKCS#12 file

4.3.3 Importing certificates and keys into storage files