Dmytro Sotnyk

Hadoop Security Project

Recommendations on TLS Certificates

2016

This documents is the summary of recommendations to TLS/SSL certificate generation procedure, signing process and server configuration.

Certificate type (asymmetric encryption algorithm)

ECC recommended, RSA acceptable

Both RSA and ECC are acceptable, but **ECC preferred** because of:
- performance
- wide industry usage
- active development

Materials:

- **Marketing Systems Hadoop Security 2016 - Asymmetric Encryption Algorithms overview**
- **Symantec: Elliptic Curve Cryptography (ECC) Certificates Performance Analysis**
- Microsoft: The advantages of Elliptic Curve Cryptography for Wireless Security
- Devoxx UK 2014, James McGivern: ECC vs RSA: Battle of the Crypto-Ninjas

RSA: Key length

8192 bits recommended, 4096 bits absolute minimum

Our target is long-term protection (until 2040) or top-secret level accordingly to NSA standards whatever better.

Prof. Arjen K. Lenstra and Prof. Eric R. Verheul equations (2000) - **3214** minimum
Prof. Arjen K. Lenstra updated equations (2004) - **2644** minimum
Network Working Group RFC3766 (2004) - **2783** minimum
ECRYPT II Recommendations (2012) - **3248** minimum
NIST Recommendations (2012) - **7680** minimum
ANSSI Recommendations (2014) - **3072** minimum
NSA Suite B cryptography (2015) Top Secret, FIPS 186-4 - **3072** minimum
BSI Recommendations (2015) - **3072** until 2021 only

Materials:

- **Marketing Systems Hadoop Security 2016 - Asymmetric Encryption Algorithms overview**

- ❏ BlueCrypt : Cryptographic Key Length Recommendation

ECC: Key length

384 bits minimum

Our target is long-term protection (until 2040) or top-secret level accordingly to NSA standards whatever better.

Prof. Arjen K. Lenstra and Prof. Eric R. Verheul equations (2000) - **191** minimum
Prof. Arjen K. Lenstra updated equations (2004) - **190** minimum
Network Working Group RFC3766 (2004) - **240** minimum
ECRYPT II Recommendations (2012) - **256** minimum
NIST Recommendations (2012) - **384** minimum
ANSSI Recommendations (2014) - **256** minimum
NSA Suite B cryptography (2015) Top Secret - **384** minimum
BSI Recommendations (2015) - **256** until 2021 only

Materials:

- ❏ **Marketing Systems Hadoop Security 2016 - Asymmetric Encryption Algorithms overview**
- ❏ BlueCrypt : Cryptographic Key Length Recommendation

ECC: Safe curve

P-521 (secp521r1) recommended
P-384 (secp384r1) absolute minimum

We are limited by the key length and library used (set of included curves).

For example, OpenSSL OpenSSL 1.0.1f includes
secp384r1 : NIST/SECG curve over a 384 bit prime field
secp521r1 : NIST/SECG curve over a 521 bit prime field
sect409k1 : NIST/SECG curve over a 409 bit binary field
sect409r1 : NIST/SECG curve over a 409 bit binary field
sect571k1 : NIST/SECG curve over a 571 bit binary field

sect571r1 : NIST/SECG curve over a 571 bit binary field
c2tnb359v1: X9.62 curve over a 359 bit binary field
c2pnb368w1: X9.62 curve over a 368 bit binary field
c2tnb431r1: X9.62 curve over a 431 bit binary field

See RFC 5480 on curve name references

Besides that NIST curves may be backdoored by NSA, we have official recommendations of US government, NSA Suite B Cryptography recommendations and NIST SP 800-56A specification.

P-521 was included to NIST recommendations, but wasn't included to NSA Suite B because P-384 is a match of AES-192, which was intended to be used instead on AES-256, but was declined due to hardware implementations issues, see materials, *see answer from Kevin M. Igoe, NSA on IETF in materials section.*

Materials:

- **Marketing Systems Hadoop Security 2016 - Asymmetric Encryption Algorithms overview**
- NSA Suite B Cryptography
- NIST SP 800-56A specification
- IETF, discussion of P521, answer from Kevin M. Igoe, NSA
- Mozilla discussion of P521 and Suite B Cryptography
- NIST Cryptographic Standards and Guidelines Development Process
- Schneier on Security : The NSA Is Breaking Most Encryption on the Internet

Signature algorithm

SHA-384 or more recommended

Accordingly to RFC 5758, only SHA-2 (SHA-224, SHA-256, SHA-384, and SHA-512) allowed.

Comodo (Rob Stradling, Senior Research & Development Scientist) confirmed that MS does not support SHA-224 and said that "SHA-512/224, SHA-512/256 and SHA-512/t aren't supported either. So, SHA-256, SHA-384 and SHA-512 are the algorithms that CAs should use".

NSA Suite B recommends SHA-384

NIST (2012) recommends SHA-384 or more

Materials:

- ❏ NSA Suite B Cryptography
- ❏ Mozilla Dev Security Policy : Message from Rob Stradling, Comodo
- ❏ NIST FIPS 180-4

Certificate validity time

Short-lived certificates recommended
90 days for manual update or less for automatic update

Reasons for short-lived certificates are:

- easy revocation of compromised certificates, if compromise known
- reduce the scope of data compromised if a server vulnerability is uncovered, such as HeartBleed.

In general, certificate for data-in-motion encryption need to follow same procedure as used for password rotation.

As for the validity period, there is no clear standards or statistic yet, just common industry examples. Let's Encrypt Certificate Authority (list of sponsors includes Akamai, Cisco, Google and EFF) uses 90 days and will decrease this time "once automated renewal tools are widely deployed"

Materials:

- ❏ Let's Encrypt : Why ninety-day lifetimes for certificates?
- ❏ Global Sign : The Advantages of Short-lived SSL Certificates for the Enterprise
- ❏ Towards Short-Lived Certificates

Way to issue certificate

Self-signed certificates must be avoided as non-verifiable;
Certificates, signed by a trusted CA highly recommended;
Certificates, signed with own root certificate may be used

We can issue next types of certificates:

- self-signed
- signed by a trusted Certificate Authority directly
- signed by a trusted Certificate Authority directly via chain of trust
- signed with own root certificate, which need to be added to list of trusted

Self-signed certificates are non-verifiable and must be avoided. Certificates, signed with own root certificate, which need to be added to list of trusted, will require additional effort for configuration and may lead to implicit security issues.

Way to sign certificate

Certificate signing request recommended

Disclosure or leak of Certificate Private Key will lead to disclosure of all data-in-motion, encrypted with this key.

So, private key need to be stored and transferred **with the same level of security** as data, protected with this key. Also we have to follow Principle of least privilege to reduce risks.

This means that Private Key may be generated by Certificate Authority only if:
- Private Key will be stored and transferred with the security level equal or higher than current data security level in Marketing Systems cluster;
- Certificate Authority need to decrypt data, encrypted with this Private Key

If these requirements didn't satisfied, we must use safe method of certificate signing via Certificate Signing Request.

Server settings: Protocol

TLS 1.2 strongly recommended
TLS 1.1 acceptable, only if configured properly
SSL of any version and TLS 1.0 are strongly prohibited

Materials:
- ❑ **PCI DSS Version 3.0 to 3.1**
- ❑ **NIST: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS)**

- Wikipedia: Transport Layer Security

Server settings: Cipher suite

- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384**
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  are recommended as well as any cipher suite, based on AES 128-256 symmetric algorithm and SHA384 or more MAC

- **AES CTR preferred over CBC, if available**

- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256**
  TLS_RSA_WITH_AES_256_CBC_SHA256
  TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  TLS_RSA_WITH_AES_128_CBC_SHA256
  are acceptable as a compromise against NSA Suite B Cryptography recommendations on signature

Materials:

- **Marketing Systems Hadoop Security 2016 - Recommendations on JVM SSL-TLS Cipher suites**
- **Marketing Systems Hadoop Security 2016 - Asymmetric Encryption Algorithms overview**
- **Marketing Systems Hadoop Security 2016 - Symmetric Encryption Algorithms overview**
- NSA Suite B Cryptography
- NIST SP 800-56A specification