



ERICSSON

3GPP SECURITY PROFILE UPDATE TLS, IPSEC, CERTIFICATES

ERICSSON



OVERVIEW



- › With this slide set, we want to give a heads up of our plans to update the 3GPP security profiles. Detailed information can be found in the end of the presentation.
- › SA3 is responsible for maintaining the 3GPP stage 3 security profiles for TLS, IPsec, SRTP, and certificates. The profiles are now outdated and the mandatory to implement algorithms are in many cases not only insecure but also extremely slow.
- › Ericsson aims for a significant update in Release 13 focusing on increasing both security and performance. The goal is to mandate support of secure algorithms with excellent performance (TLS 1.2, AES-GCM, ECDHE, ECDSA, SHA-2) as well as forbidding broken algorithms.
 - The affected 3GPP profiles are in TS 33.310, TS 33.210, TS 33.203, and TS 33.328, but also all specifications referring to these specifications.
- › New security protocols and cryptographic algorithms are driven by performance and latency, not just security.
- › **Time plan:**
 - **August 2015:** Discussion paper and CRs to SA3#80 in Tallinn (24 – 28 August).
 - **December 2015:** Deadline for Release 13 stage 3.

RECOMMENDED ALGORITHMS



- › The ICT industry is aligning on AES-GCM, ECDHE, ECDSA, SHA-2 as the new standard set of algorithms.
 - › Used in TLS, HTTP/2, WebRTC, IPsec, SRTP, SSH, X.509, S/MIME, etc.
- › These algorithms are secure, well-studied algorithms with excellent performance.
 - Based on, and designed by cryptographers from Belgium, Egypt, USA, Germany, Denmark, etc...
- › These algorithms are supported by most major libraries.
 - AES-GCM (and all algorithms without weaknesses) requires TLS 1.2.
 - The stable version of OpenSSL supports TLS 1.2, Suite B, and all NIST ECC curves.

Function	Algorithm	Parameters (SECRET)	Parameters (TOP SECRET)
Encryption	AES-GCM	AES-128	AES-256
Key Exchange	ECDHE	NIST Curve P-256	NIST Curve P-384
Digital Signature	ECDSA	NIST Curve P-256	NIST Curve P-384
Hashing	SHA-2	SHA-256	SHA-384

PERFORMANCE (SYMMETRIC ALGORITHMS)



- › Huge performance increases can be achieved with new AEAD algorithms.
- › AES-GCM has outstanding performance on modern processors and should be the first hand choice.
 - On constrained devices, AES-CCM may be a better choice.
 - On devices without hardware support for AES, ChaCha20-Poly1305 may be a better choice.
- › 3DES has significantly worse performance (an order of magnitude) then RC4.
- › TLS 1.2 with AES-GCM can be 100 times faster than TLS with 3DES_EDE_CBC_SHA.

Algorithm	Speed
AES_128_GCM	1909.1 MB/s
CHACHA20_POLY1305	625.2 MB/s
AES_128_CBC_SHA	573.7 MB/s
AES_256_CBC_SHA	486.6 MB/s
RC4_128_MD5	233.9 MB/s

OpenSSL speed on 2 GHz Intel Core i7

PERFORMANCE (ASYMMETRIC ALGORITHMS)



- › At the 128-bit security level, ECDSA with the P-256 curve has significantly better performance than RSA in use cases where both signing and verification is needed.
- › ECC has significantly smaller key sizes than RSA (256 bits compared to 3072 bits).
- › The new ECC curves (ed25519 and Ed448-Goldilocks) standardized by CFRG (ongoing work for TLS 1.3) will significantly improve the performance of ECC.
- › Asymmetric crypto is typically used for authentication and key exchange during session setup, and not for protection of traffic data.

Algorithm	Operation	Cycles
RSA-3072	Sign	$14.2 \cdot 10^6$
	Verify	$0.12 \cdot 10^6$
ECDSA (P-256)	Sign	$0.38 \cdot 10^6$
	Verify	$0.91 \cdot 10^6$
EdDSA (ed25519)	Sign	$0.06 \cdot 10^6$
	Verify	$0.19 \cdot 10^6$

Signing and verification speeds on Intel Xeon E3-1275 (59 bytes messages) <http://bench.cr.yp.to/results-sign.html>



KEY SIZE REQUIREMENTS (NIST)

- › Key length is an important security parameter, and the strength of algorithms are measured by their effective key length (e.g. RSA-2048 provides 112 bit security).
- › NIST publishes the most comprehensive list on minimum key size requirements (SP 800-57) that also considers legacy deployments (i.e. SHA-1** in the table below).
- › A good overview of SP 800-57 is given by www.keylength.com

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Key	Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
2010 (Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

COMMON ALGORITHMS AND PROTOCOLS



- › Many common algorithms and protocols have significant security flaws that can be practically exploited.
- › Algorithms with known weaknesses should be forbidden to use (red). Algorithms that cannot be forbidden should be phased out: not recommended to use and possible to disable (orange).

Scheme	Strength	Ericsson Recommendation
MD2	Totally Broken	Shall be forbidden
MD5	Totally Broken	Shall be forbidden
SSLv3	Totally Broken	Shall be forbidden
RC4	Totally Broken	Shall be forbidden
SHA-1	Broken	Shall be phased out
TLS 1.0, TLS 1.1	Broken	Shall be phased out
CBC	Broken	Shall be phased out
HMAC-MD5	Nearly Broken	Shall be phased out
RSA-1024	80	Shall be phased out
3DES (two key)	80	Shall be phased out
3DES (three key)	112	(Extremely slow)
RSA-2048	112	(Slow, Large keys)
HMAC-SHA1	128	(Often confused with SHA-1)

3GPP SECURITY PROFILES (REL-13)

ERICSSON GENERAL RECOMMENDATIONS



- › Major update of the 3GPP security profiles for TLS, IPsec, SRTP, and certificates aiming at improved security, performance, and reliability, while limiting the number of must and should implement algorithms.

- › Goal is 128-bit security everywhere with support for 256-bit security. For compatibility with legacy releases, this is not possible short term.
 - Standards should mandate implementation and recommend use of at least 128 bit security.
 - New standards and deployments should mandate use of at least 128 bit security.
 - Algorithms with known weaknesses should be removed.
 - Standards should specify and recommend implementation of algorithms for 192-256 bit security (TOP SECRET).
 - Standards should use algorithms with perfect-forward secrecy (e.g. ECDHE).
 - › This protects against leakage of long-term secrets.
 - Standards should enforce the NIST key length requirements (see e.g. www.keylength.com).
 - › Algorithms with less than 112 bit security should be forbidden to use and removed.
 - › Algorithms that cannot be removed should be not recommended and possible to disable.
 - › Algorithms with only 112 bit security can continue to be used but should not be introduced.

- › Detailed recommendations apply to both UEs and network nodes, unless otherwise stated.

3GPP SECURITY PROFILES (REL-13)

ERICSSON DETAILED RECOMMENDATIONS



› TLS / DTLS

- Mandate support of TLS 1.2 and DTLS 1.2
- Use of (D)TLS 1.0 and TLS 1.1 is not recommended.
- Use of (D)TLS 1.0 and TLS 1.1 shall be possible to disable in network nodes.
- 3GPP TLS profile should reference the TLS BCP [RFC 7525] as a whole or implement the guidelines there
 - › e.g. TLS compression and RC4 shall not be used
- May support 3DES_EDE_CBC (i.e. not mandatory to implement).
- CBC ciphersuites should not be used.
- Mandate support, preference, and recommended use of:
 - › TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (with P-256)
 - › TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (with P-256)
- Recommend support of
 - › TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (with P-384)

› SRTP

- Make a general SRTP profile for media security and Prose.
- Mandate support of AES-GCM (draft-ietf-avtcore-srtp-aes-gcm).

3GPP SECURITY PROFILES (REL-13) ERICSSON DETAILED RECOMMENDATIONS



› IPsec: IKEv2 and ESP

- Remove IKEv1 as the security profile is weak.
- Follow algorithm requirements in RFC 7321 instead of RFC 4835. Algorithms marked with "SHOULD+" must be supported. Algorithms marked with "SHOULD" may be supported.
- May support 1024-bit MODP (i.e. not mandatory to support). Use of 1024-bit MODP is not recommended. Use of 1024-bit MODP shall be possible to disable in network nodes.
- IKEv2 Configuration Payload shall be supported.
- Protocol support for High Availability [RFC6311] shall be supported.
- Mandate support, preference, and recommended use of (128-bit security):
 - › Encryption Algorithm: AES-GCM with a 16 octet ICV (with AES-128)
 - › Pseudo-random Function: PRF_HMAC_SHA2_256
 - › Diffie-Hellman Group Transform: 256-bit random ECP group
 - › IKEv2 Authentication Method: ECDSA with SHA-256 on the P-256 curve
 - › IKEv2 Hash Algorithms: SHA2-256
- Recommend support of:
 - › Encryption Algorithm: AES-GCM with a 16 octet ICV (with AES-256)
 - › Pseudo-random Function: PRF_HMAC_SHA2_384
 - › Diffie-Hellman Group Transform: 384-bit random ECP group
 - › IKEv2 Authentication Method: ECDSA with SHA-384 on the P-384 curve
 - › IKEv2 Hash Algorithms: SHA2-384

3GPP SECURITY PROFILES (REL-13)

ERICSSON DETAILED RECOMMENDATIONS



› ESP in IMS access (TS 33.203)

- Mandate support, preference, and recommend use of AES-GCM (with AES-128):
- May support DES-EDE3-CBC (i.e. not mandatory to support).
- Use of DES-EDE3-CBC shall be possible to disable in network nodes.

› Certificates profile (Applies to both (D)TLS and IKEv2)

- ECDSA shall be supported and is recommended for new certificates. ECDSA certificates shall use at least 256-bit keys (128-bit security). 384-bit keys shall be supported.
- New RSA certificates shall use at least 2048-bit keys (112-bit security). 3072-bit (128-bit security) shall be supported. 1024-bit keys (80-bit security) are not recommended and shall not be used in new certificates. Use of 1024-bit keys shall be possible to disable in network nodes.
- SHA-1 (less than 80-bit security) is not recommended and shall not be used in new certificates. Use of SHA-1 shall be possible to disable in network nodes.
- MD2 (no security) shall not be used.

› CRL profile (Applies to both (D)TLS and IKEv2)

- ECDSA shall be supported and is recommended for new CRLs. ECDSA CRLs shall use at least 256-bit keys (128-bit security). 384-bit keys shall be supported.
- SHA-1 (less than 80-bit security) is not recommended and shall not be used in new CRLs. Use of SHA-1 shall be possible to disable in network nodes.
- MD2 (no security) shall not be used.

ABBREVIATIONS



- › AES: Advanced Encryption Standard
- › BCP: Best Current Practice
- › CCM: Counter with CBC-MAC
- › CFRG: Crypto Forum Research Group (IRTF)
- › CRL: Certificate Revocation List
- › DTLS: Datagram Transport Layer Security
- › ECC: Elliptic Curve Cryptography
- › ECDSA: Elliptic Curve DSA
- › EdDSA: Edwards-curve Digital Signature Algorithm
- › ESP: Encapsulating Security Payload
- › GCM: Galois Counter Mode
- › IKE: Internet Key Exchange
- › MODP: Modulo p , where p is prime
- › SHA: Secure Hash Algorithm
- › SNI: Server Name Indication
- › SRTP: Secure Real-time Transport Protocol
- › TLS: Transport Layer Security



ERICSSON