EUROPEAN
COMMISSION

Brussels, 22.3.2019
C(2019) 2346 final

IT technical standard

Transport Layer Security (TLS)

CONTENTS

1. INTRODUCTION

This technical standard sets out the technical parameters relating to the use of the transport layer security (TLS) security protocols that are authorised for implementation on Commission systems and infrastructures, including (but not only) web servers, proxies, reverse proxies and specialised cryptographic hardware.
The fact that the technical parameters or algorithms specified here are authorised for use does not necessarily imply that all of them are exhaustively supported by DIGIT infrastructure and services. Particular vendor and technical solution implementations and evolution at DIGIT mean that it is quite possible that only a specific subset is supported. System owners requiring integration of their information systems with DIGIT components while using the TLS protocols are strongly advised to consult the DIGIT service catalogue for the particular parameters and algorithms supported at DIGIT before making design and/or product acquisition decisions.

2. SCOPE

In the scope of this document, the data to be protected by TLS protocols are restricted to unclassified data and do not include EU classified information (EUCI) data. Consequently, this document applies to data of 'publicly available', 'Commission use' and 'sensitive non-classified' confidentiality levels[1]. The Internet Engineering Task Force (IETF) has now prohibited use of the secure sockets layer (SSL), the predecessor of TLS. As technical parameters found in certificates (e.g. certificate signature algorithms, certificate validity timeframes, key usages) are enforced by the certificate profile used by the issuing CA (certificate authority), they are considered to be outside the scope of this document.
This document does not cover cryptographic key management issues. TLS implementations are expected to comply with the key management section of the standard on cryptography and public key infrastructure [4].
The recommendations here apply only to the protection of data in motion in TLS-based secure channels; they may be unsuitable for other purposes, including (but not only) long-term data confidentiality or integrity protection and digital signatures.

3. EXCEPTIONS

This technical standard is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision (EU, Euratom) 2017/8841 (Implementing Rules for Commission Decision (EU, Euratom) 2017/46[2]).

4. DEFINITIONS

For the purposes of this standard, in addition to the definitions in Article 2 of Decision (EU, Euratom) 2017/46 and Article 2 of Commission Decision (EU, Euratom) 2017/8841, the following definitions also apply:

TERM	DEFINITION
transport layer	TLS is a cryptographic protocol that provides communications security over a

[1] Previously 'public', 'limited basic' and 'limited high'.
[2] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

Tel. +32 22 991 111 Office: B-28 03/09 — Tel. direct line +32 229-56 867
ken.ducatel@ec.europa.eu

security (TLS)	computer network. Several versions of the protocols find widespread use in applications such as web browsing, mail, instant messaging and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers.
cipher	Cipher is an algorithm for encryption or decryption — a series of well-defined steps that can be followed as a procedure.
Cipher suite	It's a set of algorithms which helps secure a network connection that uses Transport Layer Security (TLS).
certificates	An SSL (secure) certificate is a file installed on a secure web server that identifies a website. This digital certificate establishes the identity and authenticity of the website, so that online users can trust that it is secure and reliable.
perfect forward secrecy (PFS)	PFS is a property of secure communication protocols in which compromises of long-term keys do not compromise past session keys. It protects past sessions against future compromises of secret keys or passwords. If it is used, encrypted communications and sessions recorded in the past cannot be retrieved and decrypted should long-term secret keys or passwords be compromised in the future, even if the adversary actively interfered, e.g. via a man-in-the-middle attack.

5. TLS IN NEWLY DEVELOPED INFRASTRUCTURES AND SYSTEMS

All modern browsers now support PFS, so implementing only ciphersuites that provide PFS must be the default TLS implementation for newly developed infrastructures and systems, provided that this is not prevented by any constraints (e.g. compatibility issues with TLS/SSL clients). Exceptions to practices set out in this document must be documented and periodically re-assessed, with a view to achieving full compliance.

6. TLS GENERAL REQUIREMENTS

6.1. Certification authorities

(M=mandatory, R=recommended)

SN	Requirement	Implementation
1.	Entities involved in setting up TLS connections shall be configured to ensure that they send their own (end-entity) certificate[3] and all certificates appearing in their certification chain, excluding the top-level self-signed (root CA) certificate.	M

6.2. Protocol versions and features

6.2.1. Authorised protocol versions

The following protocol versions are authorised, in decreasing order of preference: TLS v1.3, TLS v1.2, TLS v1.1.

(M=mandatory, R=recommended)

SN	Requirement	Implementation
2.	TLS v1.3 shall be enabled for the web browsers that support it.	M

[3] HR.DS provides guidance on using trusted certificate authorities for the applications.

3.	TLS v1.2 **shall** be the main protocol, as it offers modern authenticated encryption (authenticated encryption with associated data (AEAD)).	M
4.	TLS v1.1 **should** be used only in the absence of backwards compatibility issues.	R
5.	Only the most secure authorised protocol version **should** be used, minimising the number of supported protocol versions, e.g. having systems supporting only TLS v1.2 would be preferable to having the same systems supporting TLS v1.2 and TLS v1.1.	R

6.2.2. Unauthorised protocol versions

(M=mandatory, R=recommended)

SN	Requirement	Implementation
6.	SSL v2 **shall not** be used. It is insecure and can be used to attack RSA keys and sites with the same name, even if they are on an entirely different server (DROWN attack).	M
7.	SSL v3 **shall not** be used. It is insecure when used with http (POODLE attack) and weak when used with other protocols.	M
8.	TLS v1.0 **shall not** be used. Its major weakness (BEAST) has been mitigated in modern browsers, but other problems remain.	M

6.2.3. Features

(M=mandatory, R=recommended)

SN	Requirement	Implementation
9.	TLS renegotiation **shall** be disabled.	M
10.	TLS compression **shall** be disabled.	M
11.	Clients that 'fall back' to lower versions of the protocol after the server rejects higher versions **shall not** fall back to SSL v3 or earlier.	M

7. TLS GROUPING

Three groups[4] could be introduced to address compatibility issues between the server and the client:

- **group A** is for services that do not need backward compatibility. The parameters of this group ensure a higher level of security. Protocols: TLS v1.2;
- **group B** is for services that do not need compatibility with legacy clients (mostly WinXP), but still need to support a wide range of clients. Protocols: TLS v1.2, TLS v1.1 and TLS v1; and
- **group C** is for services that work with all clients back to Windows XP/IE6. Protocols: TLS v1.2, TLS v1.1, TLS v1 and SSL v3.

(M=mandatory, R=recommended)

SN	Requirement	Implementation
12.	Group A ciphers **shall** be used, as these are the latest and strongest.	M
13.	Group B ciphers **should** be used for compatibility issues.	R

[4] See Annex.

Tel. +32 22 991 111 Office: B-28 03/09 — Tel. direct line +32 229-56 867
ken.ducatel@ec.europa.eu

14.	Group B ciphers SHA-1 and TLS v1 **shall** be phased out for https.	M
15.	Group C ciphers **shall** be used only by an exception request and only to address compatibility issues on external-world facing systems. In the absence of compatibility issues, they **shall not** be used.	M
16.	Group C insecure or older ciphers based on RC2, RC4, DES, MD4, MD5, EXP, EXP1024, AH, ADH, aNULL, eNULL, SEED or IDEA **shall not** be used.	M

8. TLS IN EXISTING INFRASTRUCTURES AND SYSTEMS

Existing infrastructures and systems must be configured to achieve full compliance with practices set out in this document, provided that this is not prevented by any constraints (e.g. compatibility issues with TLS clients). The implementation only of ciphersuites that provide PFS is encouraged. Exceptions to practices set out in this document must be documented and periodically re-assessed with a view to achieving full compliance.

9. TLS ASYMMETRIC CRYPTOGRAPHY ALGORITHMS

9.1. Key-exchange and key-agreement algorithms

(M=mandatory, R=recommended)

SN	Requirement	Implementation
17.	The following algorithms **shall** be used:	M
17.a.	– ephemeral elliptic curve Diffie-Hellman (ECDHE) *(groups A & B)*	
17.b.	– ephemeral Diffie-Hellman (DHE) *(groups B & C)*	
17.c.	– Rivest, Shamir, Adleman public-key cryptosystem (RSA) *(group C)*	

9.2. Peer-authentication algorithms

(M=mandatory, R=recommended)

SN	Requirement	Implementation
18.	The following algorithms **shall** be used:	M
18.a.	– elliptic curve digital signature algorithm (ECDSA) *(groups A & B & C)*	
18.b.	– Rivest, Shamir, Adleman public-key cryptosystem (RSA) *(groups A & B & C)*	
18.c.	– digital signature standard (DSS) (based on the digital signature algorithm (DSA)) *(group C*	

10. TLS SYMMETRIC CRYPTOGRAPHY ALGORITHMS

(M=mandatory, R=recommended)

SN	Requirement	Implementation
19.	The following algorithms **shall** be used:	M
19.a.	– advanced encryption standard (AES): AES-256 and AES-128 *(groups A & B & C)*	

19.b.	– ChaCha20-Poly1305 *(groups A & B & C)*	
20.	ARIA and Camellia-256, Camellia-128 **should** be used as an alternative to AES in case an exception is justified for AES.	R

10.1. Block modes of operation

(M=mandatory, R=recommended)

SN	Requirement	Implementation
21.	The following modes **shall** be used:	M
21.a.	– Galois/counter mode (GCM) *(groups A & B & C)*	
21.b.	– counter with cipher-block chaining mode (CCM) *(groups A & B & C)*	
21.c.	– cipher-block chaining mode 3 (CBC 3) *(group C)*	

11. TLS HASH ALGORITHMS

(M=mandatory, R=recommended)

SN	Requirement	Implementation
22.	The following algorithms **shall** be used:	M
22.a.	– secure hash algorithm 3 (SHA-3): SHA 3-512 and SHA 3-384 *(groups A & B & C)*	
22.b.	– secure hash algorithm 2 (SHA-2): SHA-512, SHA-384 and SHA-256 *(groups A & B & C)*	
23.	The more secure 512 and 384 variants of the SHA-2 and SHA-3 algorithms **should** be implemented.	R
24.	The SHA-1 *(group C)* hash algorithm shall be used only by an exception request and only to address compatibility issues on external-world facing systems. In the absence of compatibility issues, support for it **shall** be disabled.	M
25.	Other hashing algorithms, including (but not only) the SHA-0, MD2, MD4 and MD5 algorithms, **shall not** be used.	M

12. TLS SUPPORT FOR PERFECT FORWARD SECRECY

(M=mandatory, R=recommended)

SN	Requirement	Implementation
26.	PFS **shall** be supported. This can be achieved by using ephemeral elliptic curve Diffie-Hellman (ECDHE) or ephemeral Diffie-Hellman (DHE) as a key agreement method.	M

13. TLS AUTHORISED CIPHERSUITES

(M=mandatory, R=recommended)

SN	Requirement	Implementation
27.	Ciphersuites using pre-shared keys (PSK), the secure remote password (SRP) protocol, the Kerberos protocol or any other authentication mechanisms not listed in this section	M

	shall not be used.	
28.	Ciphersuites relying on null encryption algorithms **shall not** be used.	M

Tel. +32 22 991 111 Office: B-28 03/09 — Tel. direct line +32 229-56 867
ken.ducatel@ec.europa.eu

ANNEX

Given all the requirements expressed in this document, the appropriate ciphersuites are given to the table which is in the IT Security Policy Portal [28]. Below there is a representation of this table. The ordering of a ciphersuite is very important, because it decides which algorithms will be selected as a priority. The ciphers in the table below are prioritised.

TLS ciphersuite registry values associated with each ciphersuite list are included on the basis of [21], in order to avoid confusion due to potential variations in the naming convention for different products from different vendors. The 'weak' indication is used where SHA 1 has been proven to be insecure as of 2017.

Security	Hex	Priority	Group	IANA	Key exchange or agreement	Peer auth	Symmetric cipher	Block mode of operations	Message authentication	TLS version	PFS	Hex	Alternatives to GCM mode	Hex	Alternatives to AES
Secure	0xC0,0x30	1	A	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA 384	ECDHE	RSA	AES 256	GCM	SHA 384	1.2	X			0xC0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA 384
														0xC0,0x8B	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA 384
Secure	0xC0,0x2C	2	A	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA 384	ECDHE	ECDSA	AES 256	GCM	SHA 384	1.2	X	0xC0,0xAD	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0,0x5D	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA 384
												0xC0,0xAF	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	0xC0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA 384

Secure	0xCC,0xA8	3	A	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA 256	ECDHE	RSA	CHACHA20_POLY1305		SHA 256	1.2	X				
Secure	0xCC,0xA9	4	A	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA 256	ECDHE	ECDSA	CHACHA20_POLY1305		SHA 256	1.2	X				
Secure	0xC0,0x2F	5	A	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA 256	ECDHE	RSA	AES 128	GCM	SHA 256	1.2	X			0xC0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA 256
														0xC0,0x8A	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA 256
Secure	0xC0,0x2B	6	A	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA 256	ECDHE	ECDSA	AES 128	GCM	SHA 256	1.2	X	0xC0,0xAC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0,0x5C	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA 256
												0xC0,0xAE	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	0xC0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA 256
Secure	0x00,0x9F	7	B	TLS_DHE_RSA_WITH_AES_256_GCM_SHA 384	DHE	RSA	AES 256	GCM	SHA 384	1.2	X	0xC0,0x9F	TLS_DHE_RSA_WITH_AES_256_CCM	0xC0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA 384

												0xC0,0xA3	TLS_DHE_RSA_WITH_AES_256_CCM_8	0xC0,0x7D	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA 384
Secure	0xCC,0xAA	8	B	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA 256	DHE	RSA	CHACHA20_POLY1305		SHA 256	1.2	X				
Secure	0x00,0x9E	9	B	TLS_DHE_RSA_WITH_AES_128_GCM_SHA 256	DHE	RSA	AES 128	GCM	SHA 256	1.2	X	0xC0,0x9E	TLS_DHE_RSA_WITH_AES_128_CCM	0xC0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA 256
												0xC0,0xA2	TLS_DHE_RSA_WITH_AES_128_CCM_8	0xC0,0x7C	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA 256
Secure	0x00,0xA3	10	C	TLS_DHE_DSS_WITH_AES_256_GCM_SHA 384	DHE	DSS	AES 256	GCM	SHA 384	1.2	X			0xC0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA 384
Secure	0x00,0xA2	11	C	TLS_DHE_DSS_WITH_AES_128_GCM_SHA 256	DHE	DSS	AES 128	GCM	SHA 256	1.2	X			0xC0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA 256
Secure	0x00,0x9D	12	B	TLS_RSA_WITH_AES_256_GCM_SHA 384	RSA	RSA	AES 256	GCM	SHA 384	1.2		0xC0,0x9D	TLS_RSA_WITH_AES_256_CCM	0xC0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA 384

												0xC0,0xA1	TLS_RSA_WITH_AES_256_CCM_8	0xC0,0x7B	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA 384
Secure	0x00,0x9C	13	B	TLS_RSA_WITH_AES_128_GCM_SHA 256	RSA	RSA	AES 128	GCM	SHA 256	1.2		0xC0,0x9C	TLS_RSA_WITH_AES_128_CCM	0xC0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA 256
												0xC0,0xA0	TLS_RSA_WITH_AES_128_CCM_8	0xC0,0x7A	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA 256
Secure	0xC0,0x28	14	C	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 384	ECDHE	RSA	AES 256	CBC	SHA 384	1.2	X			0xC0,0x4D	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA 384
Secure	0xC0,0x24	15	C	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA 384	ECDHE	ECDSA	AES 256	CBC	SHA 384	1.2	X			0xC0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA 384
Secure	0xC0,0x27	16	C	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 256	ECDHE	RSA	AES 128	CBC	SHA 256	1.2	X			0xC0,0x4C	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA 256
Secure	0xC0,0x23	17	C	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA 256	ECDHE	ECDSA	AES 128	CBC	SHA 256	1.2	X			0xC0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA 256

Tel. +32 22991111 Office: B-28 03/09 — Tel. direct line +32 229-56867
ken.ducatel@ec.europa.eu

Weak	0xC0,0x14	18	C	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE	RSA	AES 256	CBC	SHA	1.2	X			0xC0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA 384
Weak	0xC0,0x0A	19	C	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE	ECDSA	AES 256	CBC	SHA	1.2	X			0xC0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA 384
Weak	0xC0,0x13	20	C	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE	RSA	AES 128	CBC	SHA	1.2	X			0xC0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA 256
Weak	0xC0,0x09	21	C	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE	ECDSA	AES 128	CBC	SHA	1.2	X			0xC0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA 256
Secure	0x00,0x67	22	C	TLS_DHE_RSA_WITH_AES_128_CBC_SHA 256	DHE	RSA	AES 128	CBC	SHA 256	1.2	X			0xC0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA 256
Weak	0x00,0x33	23	C	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE	RSA	AES 128	CBC	SHA	1.0	X			0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
Secure	0x00,0x40	24	C	TLS_DHE_DSS_WITH_AES_128_CBC_SHA 256	DHE	DSS	AES 128	CBC	SHA 256	1.2	X			0xC0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA 256

Tel. +32 22991111 Office: B-28 03/09 — Tel. direct line +32 229-56867
ken.ducatel@ec.europa.eu

Secure	0x00,0x6B	25	C	TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256	DHE	RSA	AES 256	CBC	SHA 256	1.2	X			0xC0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA 384
Weak	0x00,0x38	26	C	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE	DSS	AES 256	CBC	SHA	1.0	X			0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
Weak	0x00,0x39	27	C	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE	RSA	AES 256	CBC	SHA	1.0	X			0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
Secure	0x00,0x3D	28	C	TLS_RSA_WITH_AES_256_CBC_SHA 256	RSA	RSA	AES 256	CBC	SHA 256	1.2					
Secure	0x00,0x3C	29	C	TLS_RSA_WITH_AES_128_CBC_SHA 256	RSA	RSA	AES 128	CBC	SHA 256	1.2				0xC0,0x3C	TLS_RSA_WITH_ARIA_128_CBC_SHA 256
Weak	0x00,0x35	30	C	TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES 256	CBC	SHA	1.2				0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
Weak	0x00,0x2F	31	C	TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES 128	CBC	SHA	1.2				0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

Secure	0x00,0x6A	32	C	TLS_DHE_DSS_WITH_AES_256_CBC_SHA 256	DHE	DSS	AES 256	CBC	SHA 256	1.2	X					
Weak	0x00,0x32	33	C	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE	DSS	AES 128	CBC	SHA	1.0	X			0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	

Tel. +32 22991111 Office: B-28 03/09 — Tel. direct line +32 229-56867
ken.ducatel@ec.europa.eu

REFERENCES

[1] IETF, *RFC 7525: Recommendations for secure use of transport layer security (TLS) and datagram transport layer security (DTLS)* [online]; http://www.ietf.org/rfc/rfc7525.txt

[2] IETF, *RFC 5289: TLS elliptic curve cipher suites with SHA-256/384 and AES Galois counter mode (GCM)* [online]; http://www.ietf.org/rfc/rfc5289.txt

[3] ENISA, *Algorithms, key size and parameters report — 2014* [online]; https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014

[4] HR.DS, *Standard on cryptography and public key infrastructure* [online]; https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_crypto.doc

[5] D. Giry, *BlueKrypt — Keylength — cryptographic key length recommendation* [online] http://www.keylength.com/

[6] Qualys, *Qualys SSL Labs: TLS/SSL deployment best practices* [online]; https://www.ssllabs.com/projects/best-practices/

[7] IETF, *RFC 2246: The TLS protocol version 1.0* [online]; http://www.ietf.org/rfc/rfc2246.txt

[8] IETF, *RFC 3268: Advanced encryption standard (AES) ciphersuites for transport layer security (TLS)* [online]; http://www.ietf.org/rfc/rfc3268.txt

[9] IETF, *RFC 4346: The transport layer security (TLS) protocol version 1.1* [online]; http://www.ietf.org/rfc/rfc4346.txt

[10] IETF, *RFC 4492: Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS)* [online]; http://www.ietf.org/rfc/rfc4492.txt

[11] IETF, *RFC 5246: The transport layer security (TLS) protocol version 1.2* [online]; http://www.ietf.org/rfc/rfc5246.txt

[12] IETF, *RFC 5288: AES Galois counter mode (GCM) cipher suites for TLS* [online]; http://tools.ietf.org/rfc/rfc5288.txt

[13] IETF, *RFC 6460: Suite B profile for transport layer security (TLS)* [online]; http://www.ietf.org/rfc/rfc6460.txt

[14] IETF, *RFC 6655: AES-CCM cipher suites for transport layer security (TLS)* [online]; http://tools.ietf.org/rfc/rfc6655.txt

[15] D.J. Bernstein and T. Lange, *SafeCurves: choosing safe curves for elliptic-curve cryptography* [online]; http://safecurves.cr.yp.to/

[16] Symantec, *Executive brief: Perfect forward secrecy – the next step in data security* [online]; http://resources.idgenterprise.com/original/AST-0116933_Symantec_SY002_BRF_TLSforwardsecrecy_DESIGN_V008_FINAL.PDF

[17] Qualys, *Qualys SSL Labs: Deploying forward secrecy* [online]; https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy

[18] Qualys, *Configuring Apache, Nginx, and OpenSSL for forward secrecy* [online]; https://community.qualys.com/blogs/securitylabs/2013/08/05/configuring-apache-nginx-and-openssl-for-forward-secrecy

[19] Symantec, *Introducing algorithm agility: ECC and DSA* [online]; http://www.symantec.com/connect/blogs/introducing-algorithm-agility-ecc-and-dsa

[20] Qualys, *Qualys TLS/SSL server test* [online]; https://www.ssllabs.com/ssltest/

[21] Internet Assigned Numbers Authority (IANA), *TLS ciphersuite registry* (29 February 2016) [online]; http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4

[22] IETF, *RFC 6066: Transport layer security (TLS) extensions – extension definitions* [online]; http://www.ietf.org/rfc/rfc6066.txt

[23] OpenSSL, *Wiki: Diffie-Hellman* [online]; http://wiki.openssl.org/index.php/Diffie_Hellman

[24] IETF, *RFC 5932: Camellia ciphersuites for TLS* [online]; http://tools.ietf.org/rfc/rfc5932.txt

[25] IETF, *RFC 6367: Addition of the Camellia ciphersuites to transport layer security (TLS)* [online]; http://tools.ietf.org/rfc/rfc6367.txt

[26] IANA, *Transport layer security (TLS) parameters* [online]; https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

[27] F. Weimer, *Factoring RSA keys with TLS perfect forward secrecy* [online]; https://people.redhat.com/~fweimer/rsa-crt-leaks.pdf

[28] DIGIT IT security policy portal, *TLS/SSL security standard* [online]; http://www.cc.cec/wikis/pages/viewpage.action?pageId=316507946

[29] IETF, *The transport layer security (TLS) protocol version 1.3* [online]; https://tools.ietf.org/html/draft-ietf-tls-tls13-28

[30] IETF, *Protocol action: The transport layer security (TLS) protocol version 1.3 to proposed standard (draft-ietf-tls-tls13-28.txt)* [online]; https://www.ietf.org/mail-archive/web/ietf-announce/current/msg17592.html

Tel. +32 22991111 Office: B-28 03/09 — Tel. direct line +32 229-56867
ken.ducatel@ec.europa.eu