European Maritime Safety Agency

Meeting: 26th SafeSeaNet Group Meeting

Place and date: Lisbon, 19 October 2016

Agenda item: Upgrading EMSA's PKI to support SHA-2

Document number: SSN 26.4.4

Submitted by EMSA

Summary	This document presents the upgrade path of the EMSA PKI, and specifically how this will impact the SSN request/response mechanism.
Action to be taken	As per paragraph 4
Related documents	SSN 25.6.1 - Changes in EMSA's Public Key Infrastructure

1. Background

The EMSA Public Key Infrastructure (PKI) service, which was established at SSN 15 in order to allow two-way SSL authentication, was set-up using SHA-1 as its cryptographic hash function[1]. However, this algorithm has been deprecated, in particular with respect to digital certification. The protection offered by SHA-1 SSL certificates is presently considered weak, and a global move is underway to replace SHA-1 with the SHA-2 family of hashes.

EMSA aims to have the entire SafeSeaNet system (i.e. all national and central applications, AIS providers and relevant 3rd parties) using SHA-2 by the end of 2017.

2. Current Status

EMSA has developed a completely new certificate authority (CA) which is supported by higher secure hashing standards. During this process, a new root CA certificate was created which will trust all future certificates generated by EMSA. Stakeholders who connect to an EMSA hosted application will be required to install this new root CA, as well as forthcoming client and server certificates, in order to continue exchanging information.

Secondly, a new certificate distribution point and a revocation list have been made available.

Also, the MSS has conducted successful tests in the SSN Training environment with some Member States (MSs), and the scope now needs to be enlarged to encompass all systems connected to SSN.

---

[1] A mathematical algorithm that converts any given data input into a hashed output in a one-way fashion

3. Migration Phases

Installation of the new root and intermediate bundles

In the coming months, stakeholders will be contacted by the MSS in order to ensure that the new CA root and intermediate certificates are installed and configured. For this purpose, and to allow maximum compatibility with the current version, a combined CA bundle has been created which can substitute the existing one. This bundle contains the current SHA-1 root and intermediate certificates, as well as the new SHA-2 versions, so this approach should guarantee a smooth transition to full SHA-2.

The MSS will support the distribution and configuration with each individual MS, and it is strongly suggested that the migration path should be tested in the SSN Training environment.

When the bundles have been installed in each of the MS national systems (projected before the end of 2016), the roll-out of new certificates will begin, and a calendar proposing the timeframe is attached in the annex.

SHA-1 to SHA-2 migration steps

The complete migration from SHA-1 to SHA-2 comprises the following steps:

1. EMSA and MSs install the new CA bundle at the existing SSN endpoints.
2. MSs install SHA-2 client certificates
3. MSs install SHA-2 server certificates
4. EMSA verifies that all MSs have installed the combined CA bundle before continuing
5. EMSA installs the SHA-2 server certificate
6. EMSA installs the SHA-2 client certificate

The migration will be done in three stages.

Phase 1

- Distribution and installation of the new CA bundles (by end 2016)

Phase 2

- Installation of SHA-2 client and server certificates by MSs (by end Q3 2017)
- One MS per week (as per proposed calendar)

Phase 3

- Installation of SHA-2 server certificate by EMSA (+ connection tests)
- Installation of SHA-2 client certificate by EMSA (+ connection tests)
- Process to begin after summer recess (preferably no later than 1st October)

It should be noted that the switching of the EMSA client certificate (from SHA-1 to SHA-2) might result in outages in MSs which have not correctly installed the CA bundle. These will be dealt with on a case-by-case, by both the MSS and the MS concerned, in order to minimise the downtime.

Based on the experience gained with the 2-way SSL project in 2011, a substantial success ratio is anticipated (e.g. 80/20).

4. Actions required

MSs are invited to prepare themselves for the migration by:

- ensuring that their environments will support SHA-2 certificates (a SHA-2 compatibility chart featuring most popular application servers and proxies is attached in the annex);
- drawing up an inventory of all EMSA signed certificates (listing by serial number - the MSS will make reference to this number);
- verifying the key length of their private keys (the new CA only supports RSA 2048 bit and stronger. Existing private keys can be reused, but if less than 2048 bit, should be recreated);
- creating the new certificate signing requests (CSRs) in advance to mitigate waiting times for contractors, ICT departments, etc. (the CSR file is not validated before it is signed by the CA, so it can easily be provisioned beforehand), and;
- ensuring that the new certificate revocation list (CRL) endpoint can be reached (some MSs limit their outgoing connections to the SSN endpoint only. Member States should verify whether the CRL endpoint can also be reached by their SSL terminators. See Annex for more details).

Annex

CA bundles and Certificate Revocation List (CRL)

The combined CA bundle consists of the following certificates:

SHA-1 bundle

- the classic multi-purpose bundle currently in use for all maritime applications in all environments (prod, train, dev, ..)
- single intermediate certificate
- 2048 bit public keys / SHA-1
- CA expiration 21/03/2019

SHA-2 bundle

- entire new root CA and several intermediates were created
- different intermediate per environment (prod, train, dev, ..)
- 4096 bit public keys / SHA-256
- CA expiration 20 years for root, 10 for intermediates (respectively 2036 and 2026)

A new permanent distribution point for root and intermediate certificates, CA bundles, revocation lists and the CPS documents has been set up. Under the fqdn http://emsa.europa.eu/pki/ a folder structure was created.

Path	Stores
/pki	Root and intermediate certificates SHA-1 Root and intermediate certificates SHA-256 CA bundles SHA-256 Production environments CA bundles SHA-256 Training/Devtest environments
/pki/crl	Certificate Revocation Lists
/pki/cps	Certification Practice Statement
/pki/ocsp	Online Certificate Status Protocol application (reserved for future use)

CRL

Member States should be cautious that the CRL path is reachable on TCP port 80 by their server or appliance terminating the SSL connection. EMSA recommends using the fqdn, but for IP based filters, addresses 91.231.21**6**.7 and 91.231.21**7**.7 should be reachable to establish a handshake.

Migration steps and tests chart

The chart below shows the different steps in the migration process. As a baseline configuration, both the EMSA and MS systems need to have the combined SHA-1 and SHA-2 bundle installed at their endpoints.

#	Test scenario	OK	NOK	Remarks
1	MS starts with installation of a new client certificate. This way mutual handshake between sha-1 and sha-2 signed by different ca chains is tested. This reflects the current setup in EMSA live environment during transition. **EMSA:** SrvCert sha-1 ; CliCert sha-1 **MS:** SrvCert sha-1 ; CliCert sha-2			Initial phase, the Member State upgrades its certificates to SHA-2 The action is on MS side.
2	MS adds a new server certificate. This way mutual handshake between sha-1 and sha-2 signed by different ca chains is tested for both req/resp. **EMSA**: SrvCert sha-1 ; CliCert sha-1 **MS**: SrvCert sha-2 ; CliCert sha-2			Initial phase, the Member State upgrades its certificates to SHA-2 The action is on MS side.
3	EMSA installs a new server certificate. Handshake is tested as in previous scenario. More importantly, this tests shows if MS has correctly installed new bundle (cf. it trusts EMSA) **EMSA:** SrvCert sha-2 ; CliCert sha-1 **MS:** SrvCert sha-2 ; CliCert sha-2			Second phase, EMSA upgrades its server certificates to SHA-2 Server certificate installation will reveal if MS did correctly install the multi-purpose ca-bundle (SHA1 + SHA2)
4	EMSA installs the new client certificate. Handshake is tested as in previous scenario. Both parties use only the new ca chain now. **EMSA:** SrvCert sha-2 ; CliCert sha-2 **MS:** SrvCert sha-2 ; CliCert sha-2			Third phase, EMSA upgrades its client certificates to SHA-2 Client certificate installation will reveal if MS did correctly install the ca-chain and trusts EMSA CA Foreseen Q4 2017

SHA-2 compatibility chart

This section lists the minimum software or hardware version required for SHA-2 for most popular webservers and SSL accelerators/terminators.

Server	Minimum Server Version
4D Server	14.01+
Apache	2.0.63+ w/ OpenSSL 0.9.8o+
Cisco ASA 5500	8.4(2)+
Citrix Receiver	Varies - See PDF (FIPS 140 & SHA-2 Line)
F5 BIG-IP	10.1.0+
IBM Domino Server[1]	9.0+ (Bundled with HTTP 8.5+)
IBM HTTP Server[1]	8.5+ (Bundled with Domino 9+)
IBM z/OS	v1r10+
Java based products	Java 1.4.2+
Microsoft BizTalk	2010 w/ CU9 ; 2013 w/ CU4 ; 2013 R2 w/ CU2
OpenSSL based products	OpenSSL 0.9.8o+
Oracle Weblogic	10.3.1+
SonicOS (SonicWALL)	5.9.0.0+
WebSphere MQ	7.0.1.4+

[1] IBM Domino Server by itself does not currently support SHA-2 secured connections. To use SHA-2 SSL Certificates to secure your connection, you must use an HTTP proxy server that is set up to handle your incoming HTTPS requests. Domino 9.0 includes HTTP proxy server support and is configured so that you can use it with IBM HTTP Server (https://www-01.ibm.com/support/docview.wss?uid=swg27041958).

Proposed migration calendar

Member States SHA-2 migration schedule

MS / Week	PL	ES	UK	SE	GR	NL	M	PT	EE	IT	LT	DK	SI	LV	BE	RO	NO	BG	IS	IE	CY	DE	FR	FI	HR	GI
Jan-01																										
2																										
3							🟩																			
4																					🟩					
Feb-05																										🟩
6	🟩																									
7															🟩											
8																	🟩									
Mar-09																				🟩						
10					🟩																					
11																									🟩	
12																			🟩							
13																		🟩								
Apr-14		🟩																								
15				🟩																						
16			🟩																							
17						🟩																				
May-18								🟩																		
19									🟩																	
20											🟩															
21													🟩													
22														🟩												
Jun-23										🟩																
24																						🟩				
25																								🟩		
26													🟩													
Jul-27																							🟩			
28												🟩														
29																🟩										