SSN Group meeting 26
Upgrading EMSA's PKI to support SHA-2

Agenda item 26.4.4

Joost Van Belleghem
Maritime Support Services

Lisbon / 19 October 2016

EMSA
European Maritime Safety Agency

What is SHA ?

Secure Hashing Algorithm explained

Secure Hashing is a mathematical algorithm that converts any given data input into a hashed output in a one-way manner.

This is an irreversible process and makes SHA an excellent encryption method for digital certificates.

The input (or message) is a string of variable length.

The output (or digest) has a fixed length.

What is SHA ?

SHA-1

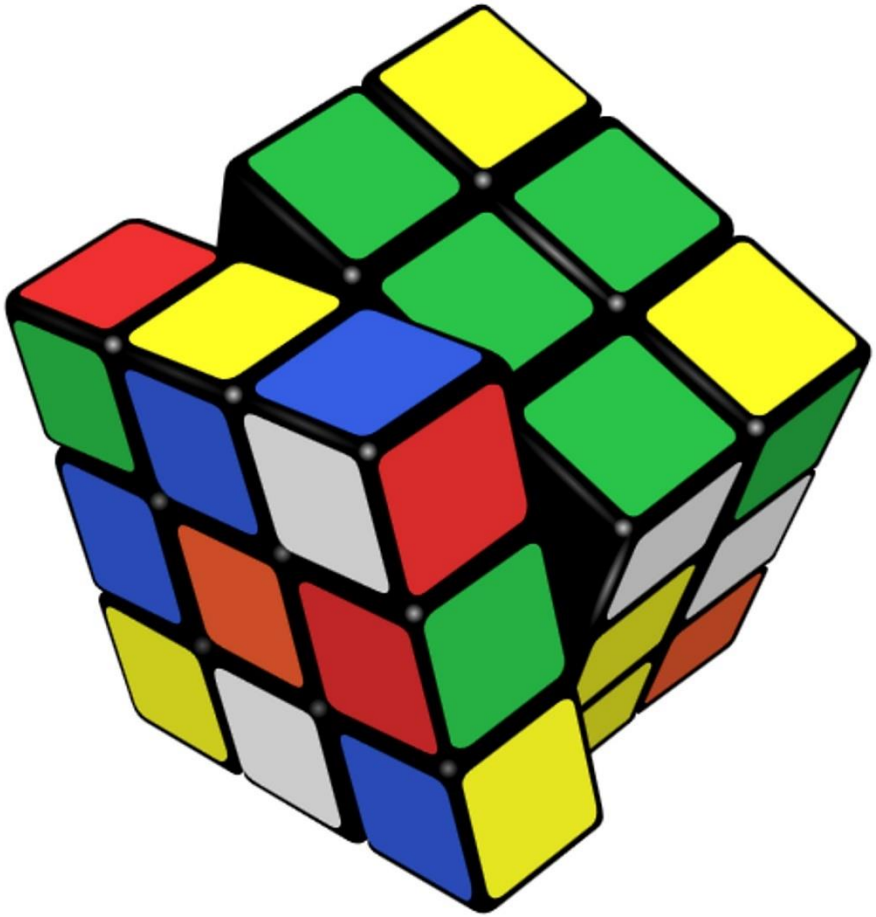
- Published in 1995
- Digest size of 160 bits
  - Ex: 30ea4d4ae99f9b9930a1306ec8ec2e4905785e2c
- Industry considers this weak in 2014
- Major players will disavow SHA-1 in 2017
  - Microsoft Internet Explorer
  - Mozilla Firefox
  - Google Chrome
  - Apple Safari

What is SHA ?

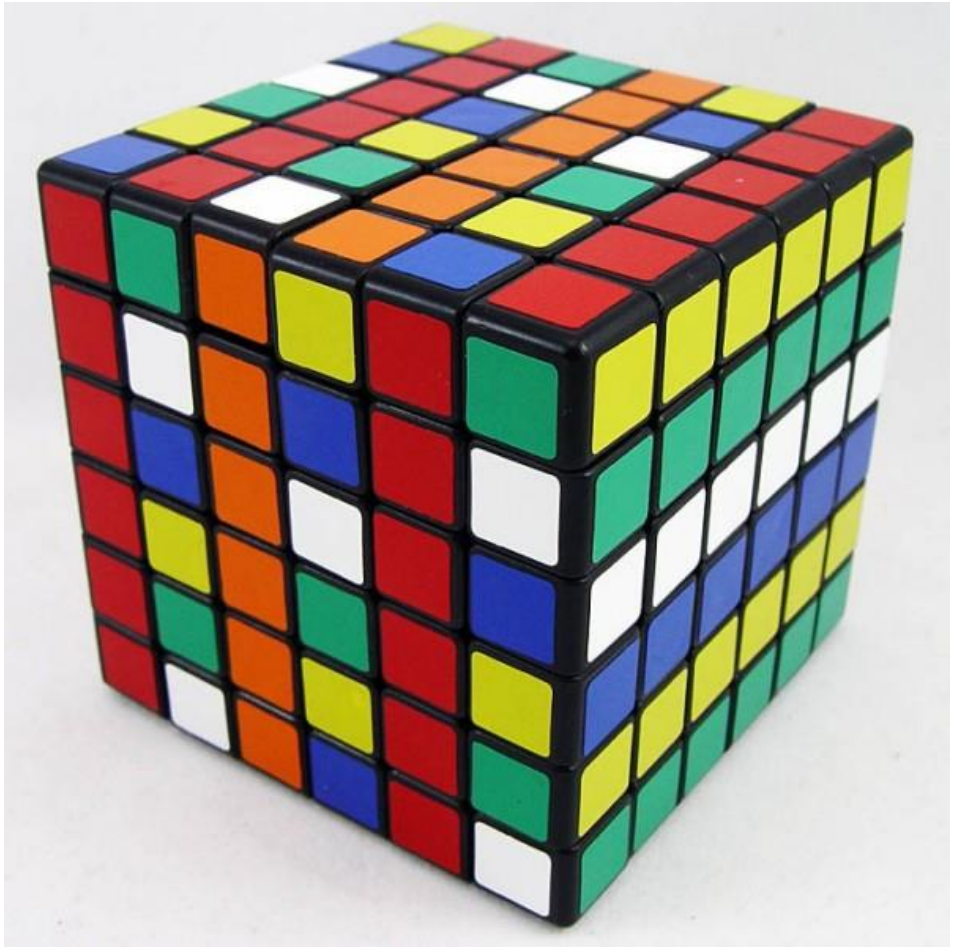
SHA-2

- Published in 2001, adopted in 2012
- Digest size of 224 to 512 bits
  - Ex 256 bit: 54c31b221ab8cc399dc7d4a5a05c838ecb48c91ad9660683480395c7dbc8f87d
- NIST recommends SHA-2 from 2014 onwards

SHA-1



SHA-2



Project Planning

Current Status

EMSA built a new CA capable of signing SHA-256 digital certificates. All current certificates will be upgraded.

The new CA has different intermediate certificates for production and training environments. This to avoid training environments to connect to production systems

Two new CA bundle were created, containing root and intermediate certificates of both current and new CA.

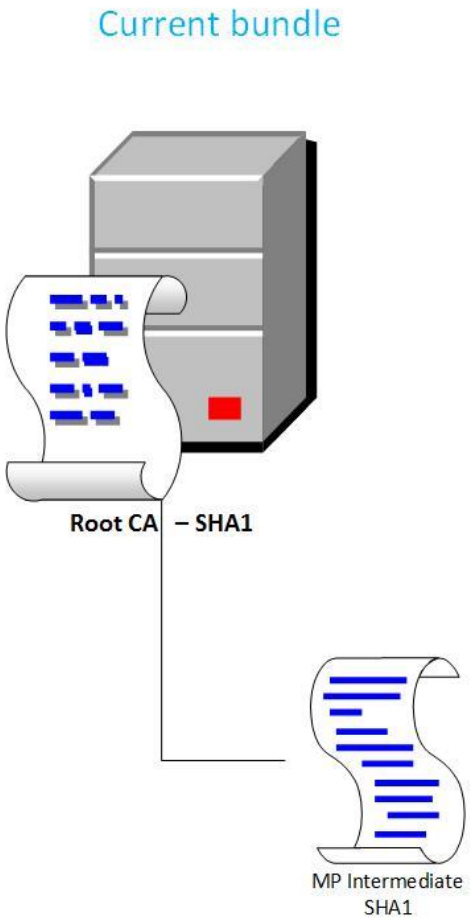
MSS will contact all MS according to the proposed migration schedule for upgrading its certificates.

Project Planning

SHA-1 bundle

The certificates currently in installed on all systems connecting to EMSA

- Contains 1 root and 1 intermediate certificate for all purposes
- 2048 bit strong
- Expires 19 March 2019



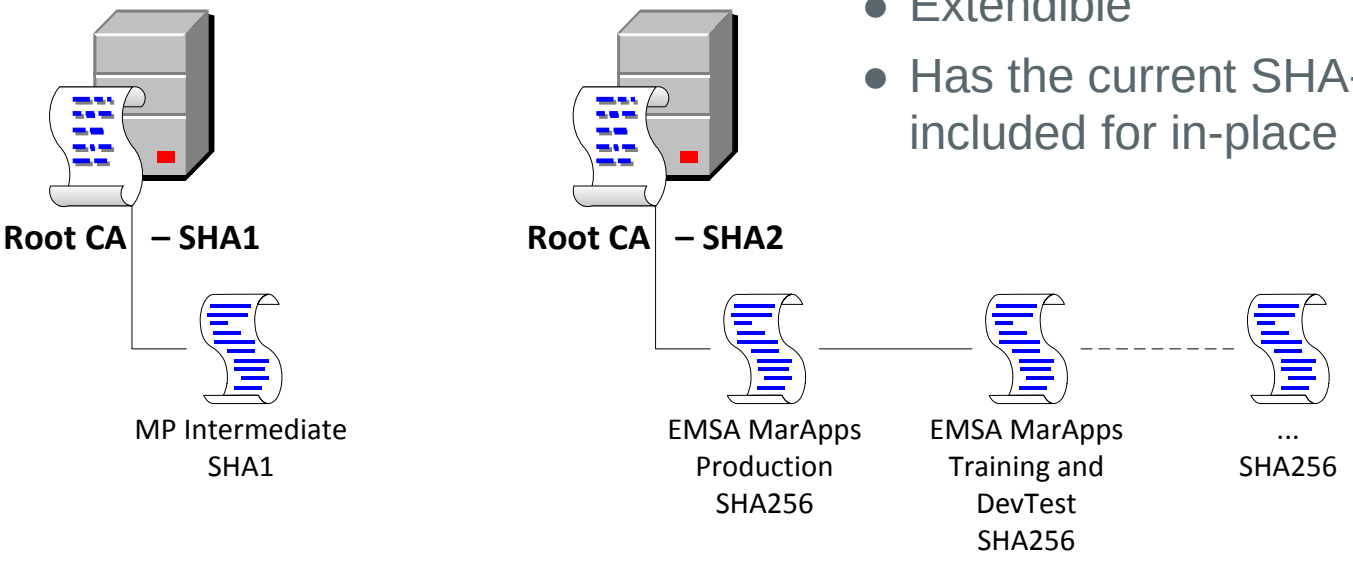
Project Planning

SHA-2 bundle

The certificates of the new CA combined with the current SHA-1 certificates

- Contains the certificates for the new new root CA and intermediate CAs
- Expires 9 May 2036
- 4096 bit strong
- Separation of Production and Training environments
- Extendible
- Has the current SHA-1 bundle included for in-place upgrade

New combined bundle



Project Planning

Migration step zero

Distribution and installation of the new CA bundles.

A permanent distribution point for EMSA PKI files has been set up under the fqdn http://emsa.europa.eu/pki/

Download the new bundles for Production and Training and install them on the SSL terminator. These bundles replace the current one.

Projected timing : Q4 of 2016

Migration steps

As from January 2017 MSS will start contacting MS for deployment of new certificates.

1. MS installs SHA-2 client certificate
2. MS installs SHA-2 server certificate
3. EMSA installs SHA-2 server certificate
4. EMSA installs SHA-2 client certificate

Project Planning

Migration steps

The migration will be broken down into two phases.

Phase 1 (target end Q3 2017)

- Installation of SHA-2 certificates by Member States
- Ratio one MS per week, as per proposed calendar

Phase 2 (as from Q4 2017)

- Installation of SHA-2 server certificate by EMSA
- Connection tests
- Installation of SHA-2 client certificate by EMSA

emsa.europa.eu

twitter.com/emsa_lisbon

facebook.com/emsa.lisbon

EMSA

European Maritime Safety Agency