SSN Group meeting 23
2-way SSL and SSN Roadmap

Agenda item 23.4.1 & 23.4.2

Marta Lima Galvão / **Senior Project Officer**
Department C: Operations/Unit C.2.2

Lisbon / 6 May 2015

EMSA
European Maritime Safety Agency

SSN 2-way SSL protocol

Introduction

- For over 5 years, the communication between central SSN and national systems has operated using the same security protocol (SSLv2/v3)
- This protocol has **effectively become obsolete**, and may affect the continuity of operations and the security of the overall SSN system (many vulnerabilities reported in 2014)
- In 2015 support to EMSA F5 security appliance ends
- In June 2014 EMSA installed a new F5 security appliance supporting more security protocols, but some backward compatibility issues with some national SSN systems arose and upgrade was suspended.
- From October 2014 a first series of tests with national SSN systems were carried out, and backward compatibility issues were isolated in 11 national SSN systems

SSN 2-way SSL protocol

NEWS

Microsoft Planning To Disable SSL 3.0 Support in December

By Kurt Mackie ■ 10/29/2014

Microsoft gave notice today that it will disable Secure Sockets Layer (SSL) 3.0 support in its Internet Explorer browser and in its Online Services, starting on **Dec. 1, 2014.**

The announcement ramps up Microsoft's earlier advice to organizations about the SSL 3.0 vulnerability by establishing a firm cut-off date. SSL 3.0 is an older encryption standard that's associated with the HTTPS method for securing Web traffic. Researchers discovered a flaw in SSL 3.0 that can be exploited to carry out so-called "man-in-th

From: LRIT [mailto:lrit@imo.org]
Sent: 31 March 2015 14:48
Subject: Communications with the DDP Server

1 In accordance with the provisions of the Technical Specifications for Communications within the LRIT System, **the DDP Server within the Production environment will utilize TLS exclusively for both incoming and outgoing connections from 1400 UTC on 7 April 2015**.

2 In particular, operators of LRIT system components should note that SSL-based communications with the DDP Server will no longer be supported. Operators are requested to confirm that operations of their respective systems are utilizing TLS for connections for all communications as provided for in the Technical Specifications to avoid any loss of communications within the LRIT system.

3 TLS support is currently enabled for the DDP Server within the Developmental Testing environment for operators who may wish to perform any testing prior to the cut-over date, after which TLS will be exclusively utilized within the Production environment.

With compliments,
LRIT@imo.org

computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

Trends

- Patch cycle becomes more time-critical

SSN 2-way SSL protocol

Proposed way forward

- Based on the answers to the questionnaire propose a date for the migration of the central SSN system to the more secure TLS protocol in **September 2015**

Action Required

- MS are invited to agree on a date for the migration of the central SSN system to the new SSL protocol

SSN v3.00 - Deployed 8 April in Production

- Changes derived from the Reporting Formalities Directive 2010/65/EU (waste and security information and improved Hazmat)
- Exchange of information on exemptions
- Changes to MRS messages
- A mechanism to ensure a transition period from SSN V2 to SSN V3
- The phase-out of Port and Hazmat request/response messages and Security notifications
- Additional minor features and changes

SSN v3.1 - link between SSN and CECIS

- SSN will automatically “push” all POLREP Incident Report messages to CECIS
- In addition, includes changes relating to the Central Ship Database
- Improvements to the web interface for consulting notifications details and creating user accounts:

- **Planned date: end of July 2015**

SSN v3.2 - STMID database

- Objective is to use SSN to simplify and facilitate the sharing of information regarding designated authorities with the Commission and other MS
- Its services will be provided through the SSN web interface as well as through the password protected section on the EMSA website

- **Planned date: before end of 2015**

emsa.europa.eu

- twitter.com/emsa_lisbon
- facebook.com/emsa.lisbon

EMSA
European Maritime Safety Agency