International Civil Aviation Organization

Thirteenth Meeting of the Common aeRonautical Virtual Private Network Operations Group (CRV OG/13)
Wellington, New Zealand, 05-08 March 2025

Agenda Item 14: Cyber-safety/security and resilience

CRV SECURITY EVOLUTIONS IN AMHS

(Presented by DSNA - France)

SUMMARY

This paper is intended to provide:

- A recap of the DSNA security context in the CRV context,
- an information about:
  - the standardization progress regarding AMHS security through the recent publication of the edition 3 of the ICAO Doc 9880 part II (end 2024),
  - the work done at different level (ICAO, Eurocontrol en Europe) to set up PKI dedicated to ANSPs.

1. INTRODUCTION

1.1 DSNA has presented different papers in previous CRV-OG meetings to address the security issue in the CRV context to be in line with its safety requirements, to protect its assets against potential cyber attacks as well as to meet the National regulation.

1.2 The importance to manage security has been mentioned by PCCW, the ANSPs and therefore by DSNA within the following papers presented in different meetings, at least:

1.2.1. IP05 "*French DNSA ai10 -CRV OG-3 DSNA Position Ver4-DSNA update*" in CRV-OG/3 (18-22 December 2017 in Bangkok).
1.2.2. WP15 "*DSNA Risk Analysis Outcome*" in CRV-OG5 (23-25 January 2019 Hong Kong)

1.3 A SAR (Security Risk Assessment) has been released to interconnect the French Polynesia and New – Caledonia network infrastructures as a basis to the CRV to exchange AMHS and Voice communication with the counterparts.

1.4 In the SAR, the security has been analyzed under the spectrum of the main items relevant to security: Availability, Integrity and Confidentiality (Authentication and Non-repudiation have not been considered).

1.5 Consequently, the main outcome of the SAR lies in the recommendation to set up encryption which could be achieved without deploying a complex global PKI thanks to network capabilities like the use of the IPSec protocols.

1.6 The use of cryptography protocols at a network level (Like IPSec) between end-to-end systems above the ICAO Regional IP network represents a significant progress to increase security and to meet the data encryption requirements derived from a SAR.

1.7 Nevertheless, in the case of aeronautical AMHS message handling systems like MTA (Message Transfer Agent), UA (User Agent) or AFTN/AMHS gateway ; it would be more suitable to use security capabilities already available in the OSI/ITU-T standards at the application level embedded in the AMHS protocol and being standardized at the ICAO level.

1.8 The goal of the document is to present:

1.8.1. The Security handling becoming more and more mature at the ICAO level particularly

1.8.2. the recent enhancement of AMHS security standardization in the ICAO Doc 9880 (edition. 3) published by the end of 2024

1.8.3. The PKI (Public Key Infrastructure) as the essential security environment requirement to set up security.

2. DISCUSSION

What should we talk about AMHS security?

2.1 A first set of AMHS security specifications were specified long time ago, they are in Doc 9880 Edition 2.

2.2 But they never were implemented operationally, notably due to lack of a common **PKI** and trust framework.

2.3 In the meantime focus on Cybersecurity has increased significantly. Without forcing implementation yet.

2.4 ICAO technical groups developed from 2017 till 2020 a significant set of AMHS security enhancements, for proposed inclusion in Doc 9880 by the ICAO Montreal Communications Panel.

2.5 These enhancements were adopted by CP/DCIWG (Communication Panel/ Data Communication Working Group) and integrated in the recently published (End of 2024) Doc 9880 Edition 3 Part II.

What is meant with “AMHS Security” in ICAO Doc 9880

2.6 “AMHS Security” in Doc 9880 Part II refers to X.400 security functionalities, implemented in the application layer.

2.7 They are implemented “above” network security (IPSec for example) and transport security (TLS for example).

2.8 They are independent of network security and transport security.

2.9 They provide:

2.9.1. **Authentication**: ensure that the communicating systems are truly “who they claim to be”

2.9.2. **Message origin authentication** : ensure that the message originator is truly “who it claims to be” (avoid spoofing)

2.9.3. **Content integrity :** ensure that the message text and data have not been modified during its conveyance.

2.10 They rely upon **asymmetric cryptography** (digital signatures) and **public key certificates (X.509)**.

The weaknesses of AMHS Security existing in the previous version of Doc 9880 (edition 2)

2.11 The majority of AMHS messages are actually the result of conversion of AFTN messages at an AFTN/AMHS gateway. Thus, this excludes to apply any kind of AMHS security protocole fields and rules, thereby creating a significant gap in the capability to implement a secure AMHS.

2.12 MTA-to-MTA connection is poorly protected (only password in clear),

2.13 UA-to-MTA connection is poorly protected.

The enhancements specified in Doc 9880 edition 3

2.14 Three major security upgrades are introduced in Edition 3:

2.14.1. Introduction of strong authentication from UA to MTA and MTA to MTA (use a cryptographic “Bind-token” instead of the current password in clear)

2.14.2. Message origin authentication and content integrity for messages generated by AFTN/AMHS Gateways (MTCU : Message Transfer and Control Unit), so as to cover 99% of the AMHS traffic

2.14.3. Update of cryptographic algorithms : Doc 9880 Edition 2 cryptographic settings were 20+ years old, they are replaced with state-of-the-art cryptographic algorithms

2.14.4. Security “good practices” and prerequisites are introduced:

2.14.4.1. Security of indirect use of AMHS in AMHS domains (AFTN terminals, AFTN to AFTN/AMHS Gateway links, etc.)

2.14.4.2. Allocation of security certificates for all components (MTAs, Gateways (MTCUs) in addition to UAs)

2.14.4.3. Logging of security errors.

Overall View

2.15 X.400-based AMHS Security…

2.15.1. Requires the provisioning of trustworthy public key certificates delivered by a commonly trusted PKI (Eurocontrol is implementing one such PKI named EACP)

2.15.1.1. A dedicated CA (Certificate Authority) is under development through EACP (European Aviation Common Public Key Infrastructure).

2.15.2. Will considerably enhance Cyber-security in the AMHS environment, when implemented

2.15.3. Is expected to become progressively a usual matter in AMHS operation

2.16 Cyber-security in the AMHS environment is not only “AMHS Security”:

2.16.1 Malware protection through Antivirus (already deployed by different ANSPs)

2.16.2 Is expected to be integrated by AMHS suppliers via software updates

2.16.2.1 To manage certificates and http protocol might be used for CRL (Certificate Revocation List) updates

2.16.3 IP and/or TCP level security

2.16.3.1 The use of security at the AMHS application level does not prevent to set up a security network architecture through firewall, Proxy…

2.16.4 system protection: logs collection, centralized maintenance staff authentication,

2.16.5 SOC (Security Operation Center).

2.16.5.1 A SOC enables the monitoring of security events and coordination between SOC of different ANSPs could be set up to investigate a security attack and to deploy appropriate protection and answer.

3. ACTION BY THE MEETING

3.1 The meeting is invited to note that:

a) The implementation of security at the application level or at least with end-to-end network encryption mechanism aside of the ICAO Regional IP network should be given the level of priority corresponding to the level of threat against organizations integrity and air traffic control safety. Security might have important impact on safety.

b) The standardization is available in the ICAO Doc 9880 to provide a high level of security for AMHS.

c) That a PKI deployment is a prerequisite to deploy AMHS security meeting the ICAO standards.

d) To note and comment the information provided in the document.

e) To decide if the importance of the subject deserves a conclusion or decision to be taken.

– – – – — – – – – – –