Aeronautical Telecommunication Network Panel (ATNP)

Working Group 2

Meeting 21

July 11 –14, 2000

Limerick, Ireland

Draft

FAA Sub-Volume V

(IDRP Authentication)

Validation Report

Presented by Tom McParland

Summary

This report presents the framework for results of the US FAA IDRP Security Validation Initiative (FAA_IDRP) that are near completion. This report follows the format of the French ATN Validation report (W2WP 578) to facilitate merging of these reports into a final report of Sub-Volume V validation. This report along with the detailed AVE reports will be presented in final form at the Working Group 1/Sub-Group 2 meeting scheduled for Atlantic City 31 July through 2 August in Atlantic City.

TABLE OF CONTENTS

1. Introduction

1.1 Purpose of the document

This report presents the results of the US FAA IDRP Security Validation Initiative (FAA_IDRP) that have been obtained in the period from December 1999 to June 2000. It summarises the outcomes of the validation exercises, lists the ATN Validation Objectives that have been covered, and finally expresses the level of confidence of the FAA on the quality and correctness of the IDRP security features as specified in Sub-Volume V.

1.2 Structure of the document

This document comprises the following sections:

- Chapter 1 is the introductory section
- Chapter 2 gives an overview of the FAA_IDRP Initiative, describes the tools used for the validation, and list the objectives
- Chapter 3 provides the status of the implementation of the draft 3rd edition ICS enhancements, and reports on the potential defects raised by the development team.
- Chapter 4 summarizes the results of the validation initiative
- Chapter 5 is the conclusion of this report

1.3 References

REF1 Proposed Draft third Edition of Doc 9705 Sub-Volume 5 (10 December 99)

REF2 Proposed Doc 9705, Sub-Volume V (ICS) 3rd Edition Validation Report

REF3 WG1/SG2 WP1907 Validation of Test Vectors for Cryptographic Functions

REF4 WG1/SG2 WP 1913 ATN PKI Lab Test Report

REF5 WG1/SG2 WP 20xx *tbsl* Validation of ATN Cryptographic Primitives in IDRP

REF6 WG1/SG2 WP 20xx *tbsl* IDRP Authentication Analysis

REF7 *tbsl* MITRE report on Validation

2. The FAA IDRP Security Validation Initiative

2.1 Introduction

The FAA IDRP Security Validation Initiative (FAA_IDRP) is the validation programme undertaken by the US Federal Aviation Administration to contribute toward the validation of the third edition of Doc 9705 Sub-Volume V.

The principle of FAA_IDRP is to implement and test the ATN cryptographic primitives in IDRP on the FAA William J Hughes Technical Center (WJHTC) ATN Router. The FAA_IDRP will verifies correct implementation of the IDRP security features in a ground-ground environment. The FAA_IDRP also includes validation through detailed analysis and inspection.

2.2 Initiative Reference & Title

FAA_IDRP: FAA IDRP Security Validation Initiative

2.3 Type

Analysis/pre-operational implementation

2.4 Responsible State/Organisation

FAA Technical Center (ACT-350)

2.5 Contact Point

State/Organisation	Contact Details
FAA Technical Center	Mr. Thomas McParland BCI/FAA ACT-350 Tel: 609-485-5929 Fax: 609-641-0203 e-mail: tjmcparland@bcisse.com

2.6 Validation tools involved

The experiments are conducted at the William J Hughes Technical Center (WJHTC) ATN interoperability test laboratory. The WJHTC ATN interoperability test laboratory consists of multiple Intel workstations running FAA ATN Router software, and which can be interconnected in multiple ways through X.25 and/or Ethernet subnetworks according to the test scenarios requirements. Two workstations are available for validation purposes; however, for test configurations that require more than 2 systems, it is possible to run multiple instances of the ATN Router software on each of the available workstations, and to interconnect each running instance of an ATN system through either real or simulated X.25 subnetworks.

The FAA ATN Router software is a re-host of the FAA's Data Link Processor (DLP) software. This software has been updated to be compliant with applicable edition 2 Doc 9705 features, in particular, support for traffic types and a network management capability have been added. The FAA ATN Router has undergone preliminary interoperability with ACIs RRI router. The FAA ATN Router is to be used for testing the ATN infrastructure as part of the FAA's CPDLC program.

2.7 Validation Period

The validation of the draft third edition of Doc 9705 Sub-Volume V spans over a period of 7 month from December 1999 to June 2000.

2.8 Objectives of the FAA IDRP Security Validation Initiative

2.8.1 General objectives of FAA_IDRP

The FAA IDRP Security Validation Initiative mainly aims at demonstrating that:

1. the authentication requirements of the third edition of Doc 9705 Sub-Volume V are implementable,

2. the authentication requirements of the third edition of Doc 9705 Sub-Volume V satisfies the user requirements as specified in Sub-Volume VIII,

3. the authentication requirements of the third edition of Doc 9705 Sub-Volume V are complete, consistent, and unambiguous.

2.8.2 Detailed Objectives

2.8.2.1 General

The overall strategy for the validation of the IDRP authentication requirements in the draft third edition of Doc 9705 Sub-Volume V has been defined by ATNP/WG2, on the basis of its past experience on the validation of the baseline edition of Doc 9705 Sub-Volume V. The starting point of the validation process is the definition by ATNP/WG2 of a common unique set of *ATN Validation Objectives (AVOs)*. AVOs are statements which express the various verifications and evaluations required in order to declare related part of the draft third edition of Doc 9705 Sub-Volume V as validated.

The coverage of AVOs by the FAA IDRP Security Validation Initiative is described in the following sections.

AVO Number	Description
AVO-3_210	Verify that ground BISs and air-ground BISs will interoperate for the secure exchange of IDRP information. The provisions to authenticate IDRP exchanges with the peer BIS across a ground-ground path will be verified.
AVO-3_211	Verify that compliant airborne and air-ground BISs supporting authentication of IDRP exchanges in the air-to-ground direction will interoperate.
AVO-3_212	Verify that compliant airborne BISs and air-ground BISs supporting the optional mutual authentication of IDRP exchanges are each able to authenticate IDRP PDUs received from the peer BIS.
AVO-3_213	Verify that compliant airborne BISs and air-ground BISs supporting the option to request and to attach a security certificate to an IDRP OPEN-PDU will interoperate.
AVO-3_214	Verify that a compliant airborne BIS, air-ground BIS and ground BIS will interoperate for the unsecured exchange of routing information with a peer BIS implemented in accordance with the current baseline Sub-Volume V provisions.

AVO-3_400	Evaluate the ground BISs and air-ground BISs capability to authenticate IDRP exchanges with the peer BIS across a ground-ground path.
AVO-3_401	Evaluate the compliant airborne and air-ground BISs capability for authentication of IDRP exchanges in the air-to-ground direction.
AVO-3_402	Evaluate the compliant airborne BISs and air-ground BISs capability for the mutual authentication (option) for IDRP exchanges.
AVO-3_403	Evaluate the security information exchange and processing overhead for the secure exchange of IDRP routing information, between ground and air-ground BISs.
AVO-3_404	Evaluate the security information exchange and processing overhead for the secure exchange of IDRP routing information, between airborne and air-ground BISs.

2.9 Validation strategy

The principle of the initiative is first to develop the ATN cryptographic primitives compliant with third edition of Doc 9705 Sub-Volume VIII and then to incorporate those primitives into an instance of an ATN router with an implementation of the applicable requirements for IDRP authentication as specified in Sub-Volume V. The system is developed independent of the specification activity, i.e., by individuals who have not participated to the production of the SARPs. This provides further level of confidence that the SARPs are complete, consistent, and unambiguous. During implementation, the FAA experts participating to the ATNP/WG2 consider any requests for clarification, or questions raised by the development team. Those issues requiring correction to Sub-Volume V or Sub-Volume VII, and/or provision of additional guidance are reported to the WG2 and/or to the CCB under the form of PDRs or of Working Papers.

Once a draft 3rd edition implementation of the cryptographic primitives and of IDRP with Type 2 authentication is completed, the focus is directed on the testing of the new functionality and the coverage of the associated AVOs. The AVOs coverage is achieved through the performance of a number of ATN Validation Exercizes (AVEs) . The problems detected with the validation exercizes are reported to the WG2 and/or to the CCB under the form of "Potential 3rd Edition Defect Reports" (P3DRs) or of Working Papers. The result of each AVE is documented in a separate AVE result report made available on the ATNP archive.

In addition to implementing IDRP Type 2 authentication, a detailed analysis and inspection of the applicable sections of Sub-Volume V and VIII is performed. This analysis is performed from two perspectives. The first view is in terms of requirements traceability. All Sub-Volume V requirements are traced back to Sub-Volume VIII requirements. This traceability analysis is intended to demonstrate that the standards and framework requirements of Sub-Volume VIII have a complete set of corresponding requirements in Sub-Volume V. The second view is in terms of operational scenarios. Operational scenarios which address air-ground and ground-ground IDRP type 2 authentication are developed. All combinations of options for local policy for Type 1 and Type 2 authentication support and for unilateral and mutual authentication, certificate availability conditions, and replay and manipulation protection are developed. The applicable Sub-Volume V requirements are then mapped into these scenarios for a complete analysis.

The FAA_IDRP summary report is produced on the basis of the outcomes of the implementation phase, the AVE result reports, and the analysis and inspection reports.

3. Implementation status and report

3.1 Implementation status

The following table summarizes the current status of the implementation IDRP security features

Item	Description	Implementation status
1	Implementation of ATN Cryptographic primitives as specified in section 8.5 of Sub-Volume VIII.	Complete Implementation
2	Requirements for enhanced IDRP security. These requirements are identified as Sub-Volume V edition 3 enhancement ICS3-06.	Partial Implementation (see below)

Status of the implementation of the version 3.0 of the ProATN Air-Ground BIS

The enhancement ICS3-6 has been partially implemented. The software implements all procedures and options related to the use of the ASVDP, AKDF, AMACP, and AMACVP procedures that are specified in Sub-Volume 8. However, implementation of procedures for negotiation of the use of mutual or single-entity authentication on air-ground IDRP connections has not been implemented.

No major deficiency has been identified on the ICS3-06 enhancements. The implementation and analysis of ICS3-06 enhancement resulted in tbsl potential defects on the third edition of of Doc 9705 Sub-Volume V. All these defects have been reported to the SubVolume V Subject Matter Expert and have been resolved by the Working Group2 by amending the draft third edition, or through the identification of items to be included as additional Guidance Material. These defects are listed by title in the table below. The associated P3DR forms are available on the ATNP archive.

P2DR number	Title
M00200xx	tbls

A number of Editorial corrections were proposed, and logged in an addendum/Corrigendum to the draft third edition of Doc 9705 until their incorporation in the final draft.

4. Validation exercises results report

4.1 Introduction

FAA_IDRP consists of the 2 ATN Validation Exercises (AVE) listed by title in the following table. These Validation Exercises are specified in [REF3]. Each exercize comprised multiple Validation Tests. For each Validation Exercise, a separate ’AVE Result report’ has been produced. These Result Reports are made available to the ATN community via the ATNP archive at the following URL

http://www.tls.cena.fr/atnp/wg1/sg2/wps

AVE name	AVE title	AVE Result report
AVE_100	Validation of ATN Cryptographic Primitives in IDRP	REF5
AVE_101	IDRP Authentication Analysis	REF6

The following sections provide a summary of the results of these exercizes.

4.2 AVE_100 results

4.3 AVE_101 results

5. Conclusion

As a result of the successful incorporation of the draft third edition enhancements to the ICS SARPs into the FAA ATN Router, and considering the success of the validation exercizes, the WJHTC is in position to express its confidence regarding the quality, and the validity of the IDRP authentication changes to Sub-Volume V of the third edition of Doc 9705.

With the exception of the procedures for negotiation of air-ground authentication options, all applicable draft 3rd edition enhancements have been implemented, and tested. It has been verified that these enhancements do not compromise the correct execution of the baseline functions of the ATN systems, and that interoperability between ATN systems is maintained. No major deficiency has been identified.

The implementation of the enhancements and the first validation exercises allowed the detection of some areas in the specification where clarifications were required. This resulted in the production of a number of defect reports the resolution of which is in progress. However, in general, the third edition of Doc 9705 SubVolume V was found consistent and unambiguous.