

|  |
| --- |
| CCSDS SECURITY CREDENTIALS Test |

DRAFT CCSDS Record

CCSDS 3XX.1-Y-1

Yellow Book

March 2018

# FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This document is therefore subject to CCSDS document management and change control procedures, which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

<http://www.ccsds.org/>

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of this publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

* Agenzia Spaziale Italiana (ASI)/Italy.
* British National Space Centre (BNSC)/United Kingdom.
* Canadian Space Agency (CSA)/Canada.
* Centre National d’Etudes Spatiales (CNES)/France.
* China National Space Administration (CNSA)/People’s Republic of China.
* Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
* European Space Agency (ESA)/Europe.
* Federal Space Agency (FSA)/Russian Federation.
* Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
* Japan Aerospace Exploration Agency (JAXA)/Japan.
* National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

* Austrian Space Agency (ASA)/Austria.
* Belgian Federal Science Policy Office (BFSPO)/Belgium.
* Chinese Academy of Sciences (CAS)/China.
* Chinese Academy of Space Technology (CAST)/China.
* China Satellite Launch and Tracking Control General, (CLTC)/China.
* Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
* Departamento De Ciência E Tecnologia Aeroespacial (DCTA)/Brazil.
* Danish National Space Center (DNSC)/Denmark.
* Electronics and Telecommunications Research Institute (ETRI)/Korea
* European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
* European Telecommunications Satellite Organization (EUTELSAT)/Europe.
* Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand
* Hellenic National Space Committee (HNSC)/Greece.
* Institute of Space Research (IKI)/Russian Federation.
* Indian Space Research Organization (ISTRAC)/India.
* Korea Aerospace Research Institute (KARI)/Korea.
* KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary
* Ministry of Communications (MOC)/Israel.
* Naval Center for Space Technology (NCST)/USA.
* National Institute of Information and Communications Technology (NICT)/Japan.
* National Oceanic and Atmospheric Administration (NOAA)/USA.
* National Space Agency of the Republic of Kazakhstan (Kazcosmos) (NSARK)/ Republic of Kazakhstan.
* National Space Organization (NSPO)/ Taiwan.
* South African National Space Agency (SANSA)/ South Africa.
* Swedish Space Corporation (SSC)/Sweden.
* Swiss Space Office (SSO)/Swiss Confederation.
* Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
* Central Research Institute of Machine Building (TsNIIMash)/ Russian Federation.
* The Scientific and Technological Research Council of Turkey (TUBITAK)/ Turkey
* United States Geological Survey (USGS)/USA.

# DOCUMENT CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | **Title and Issue** | **Date** | **Status** |
| CCSDS 000.1-R-1 | CCSDS NETWORK LAYER SECURITY ADAPTATION PROFILE, Draft CCSDS Record, Issue 1 | August 2013 | Current draft |
|  |  |  |  |
|  |  |  |  |

**Contents**

[FOREWORD 2](#_Toc475699279)

[DOCUMENT CONTROL 4](#_Toc475699280)

[1.0 Introduction 6](#_Toc475699282)

[1.1 Purpose 6](#_Toc475699283)

[1.2 Scope 6](#_Toc475699284)

[1.3 Applicability 6](#_Toc475699285)

[1.4 Rationale 6](#_Toc475699286)

[1.5 Document Structure 6](#_Toc475699287)

[1.6 References 6](#_Toc475699288)

[2.0 Overview 7](#_Toc475699289)

[3.0 Summary of interoperability and compatibility testing 8](#_Toc475699292)

[3.1 X.509 Certificates Syntax 8](#_Toc475699294)

[3.1.1 CCSDS shall implement X.509 V3 certificates 8](#_Toc475699295)

[3.1.2 The CCSDS X.509 V3 certificates shall use Generalized Time. 8](#_Toc475699296)

[3.1.3 The CCSDS X.509 V3 Certificates Shall Utilize the CCSDS Calendar Segmented Time Code (CCS), CCSDS 301.0-B-4 Time Code Formats. 8](#_Toc475699297)

[3.1.4 The CCSDS X.509 V3 Output File Format Shall Be Privacy Enhanced Mail (PEM). 8](#_Toc475699298)

[4.0 TEST details 9](#_Toc475699301)

[4.1 Certificate Validation test #1 10](#_Toc475699303)

[4.1.1 Test Description 10](#_Toc475699305)

[4.1.2 Expected Results 10](#_Toc475699307)

[5.0 INTEROPERABILITY testing between NASA and CNES 11](#_Toc475699310)

[5.1 Certificate Validation test#1 12](#_Toc475699314)

[5.2 Certificate Validation test#2 15](#_Toc475699315)

[5.3 Certificate Validation test#3 15](#_Toc475699319)

[5.4 Certificate Validation test#4 15](#_Toc475699325)

[6.0 OBSERVATIONS 16](#_Toc475699326)

**Tables**

[Table 3‑1: Test items 9](#_Toc475699515)

[Table 5‑2: X.509 Certificate Test 9](#_Toc475699516)

**Figures**

[Figure 5.1: CNES-NASA test setup 11](#_Toc475699643)

# Introduction

## Purpose

The purpose of this document is to describe the compatibility testing conducted for the CCSDS Security Credentials.

## Scope

The scope of this document is the testing results of the Security Credentials which will be implemented and used for CCSDS missions.

## Applicability

This recommendation applies to any CCSDS mission using the Security Credentials and requiring end-to-end confidentiality, authentication, or integrity from the sender to the receiver regardless of the number of intermediate hops between them.

## Rationale

Many CCSDS missions require security services to protect commanding (command authentication, command confidentiality, command integrity) and payload data (confidentiality, integrity). Missions using the Internet Protocol (IP) may also utilize link layer security.. This document discusses interoperability testing of the CCSDS profile utilizing the Credentials.

## Document Structure

This document describes the tests, configurations tested and not tested, and test results from the Credentials development and interoperability testing

## References

The following documents are informative references used to accomplish testing.

1. RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 https://www.ietf.org/rfc/rfc5280.txt
2. Time Code Formats. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 301.0-B-4. Washington, D.C.: CCSDS, November 2010.
3. Internet Security Glossary https://www.ietf.org/rfc/rfc2828.txt
4. Privacy Enhancement for Internet Electronic Mail <https://tools.ietf.org/html/rfc1424>
5. Information Security Glossary Of Terms CCSDS 350.8-G-1

# Overview

Many CCSDS missions require security services such as confidentiality, integrity, and authentication to protect spacecraft commands, software uploads, engineering telemetry, and science payload data.

# Summary of interoperability and compatibility testing

The basic digital signature interoperability test uses a minimal certificate management system structure, with a single CA, to ensure that clients have interoperable digital signature functionality and can correctly parse signatures and validate a single certificate.

The test is uses symmetrical clients with peer-to-peer relationships and involves exchanging signed messages and validation of the signatures. This test is run with a peer-to-peer digital signature application such as S/MIME.

This test is intended to test basic digital signature processing interoperability. This test is executed between CNES and NASA

## X.509 Certificates Syntax

### CCSDS shall implement X.509 V3 certificates

Note: Reference # 1

### The CCSDS X.509 V3 certificates shall use Generalized Time.

Note: Reference # 1

### The CCSDS X.509 V3 Certificates Shall Utilize the CCSDS Calendar Segmented Time Code (CCS), CCSDS 301.0-B-4 Time Code Formats.

Note: Reference # 2

### The CCSDS X.509 V3 Output File Format Shall Be Privacy Enhanced Mail (PEM).

Note: Reference # 4

# TEST details

The NASA/CNES internal testing is going to use internal on-line devices. The testing between CNES and NASA end-points is carried out over the Internet. NASA Glenn Research will utilize an externally facing host computer outside the NASA firewall to ease connectivity and provide flexibility.

CNES firewall, equipment, software and support contracts should not affect the exchange and validation of the certificates.

Table 3‑1: Test items

|  |  |
| --- | --- |
| NASA: | CNES: |
| HP ZBook #2347170 |  |
| Operating System Ubuntu 14.04 |  |
| OpenSSL |  |
| E-mail Client |  |

Table 1 Equipment and software utilized during testing.

Table 5‑2: X.509 Certificate Test

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Credential Structure | |  |  |  |
| Item # | Feature | Status | NASA | CNES |
| 1 | ASN1 | M |  |  |
| 2 | DER | M |  |  |
| 3 | X.509.V3 | M |  |  |
| 4 | tbsCertificate | M |  |  |
| 5 | Version | M |  |  |
| 6 | Serial number | M |  |  |
| 7 | algorithm identification | M |  |  |
| 8 | Issuer Signature | M |  |  |
| 9 | Validity from | M |  |  |
| 10 | Validity to | M |  |  |
| 11 | Subject | M |  |  |
| 12 | Subject algorithm identification | M |  |  |
| 13 | Subject public Key | M |  |  |
| 14 | Issuer Unique ID | O | N/A | N/A |
| 15 | Subject Unique ID Public Key Info | O | N/A | N/A |
| 16 | Universal Time Coordinated Time Certificate | M |  |  |
| 17 | Generalized Time | M |  |  |
| 18 | object identifiers (OID) | O | N/A | N/A |
| 19 | Policy Mapping | O | N/A | N/A |
| 20 | Subject Alternative Name | O | N/A | N/A |
| 21 | Certificate Revocation Lists distribution points | O | N/A | N/A |
| 22 | signatureAlgorithim | M |  |  |
| 23 | signatureValue | M |  |  |

Table 3-2 Details the Certificate structure and Options.

CNES and NASA performed local testing prior to interoperability testing.

## Certificate Validation test #1

### Test Description

Create certificates and place them on local client computers to ensure that clients have interoperable digital signature functionality and can correctly parse signatures and validate a single certificated endpoint recipient via a network connection. Then e-mail exchange of self-signed certificates between endpoints. End points place certificates in the appropriate file locations. Then encrypted e-mails are exchanged and decoded.

### Expected Results

Test e-mails will successfully be decrypted in the chosen email client using S/MIME and the peer client certificate.

# INTEROPERABILITY testing between NASA and CNES

Interoperability testing is used to measure how well software applications or hardware devices function in concert with relevant hardware, software, operating systems or network environments.



Figure 5.1: CNES-NASA test setup

Figure 5.1 is an illustration of the CNES and NASA agreed test setup. Appropriate documentation was exchanged between CNES and NASA order conduct necessary testing without decreasing security of either institution. The NASA client will be hosted outside the NASA firewall the hosted system is not connected to the internal NASA network. CNES will provide the appropriate e-mail address for their test systems client, the picture assumes that the client will be behind the CNES firewall and the encrypted e-mail will pass their packet filter as other encrypted e-mail traffic does.

Table 5‑1: Compatibility tests and results

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Certificate** | **NASA**  **Reads**  **CNES**  **Certificate** | **CNES**  **Reads**  **NASA**  **Certificate** | **Encrypted**  **E-Mail**  **Exchanged from**  **NASA to CNES** | **Encrypted**  **E-Mail**  **Exchanged from**  **CNES to NASA** | **Interoperability** |
|  | X | X | X | X | X |

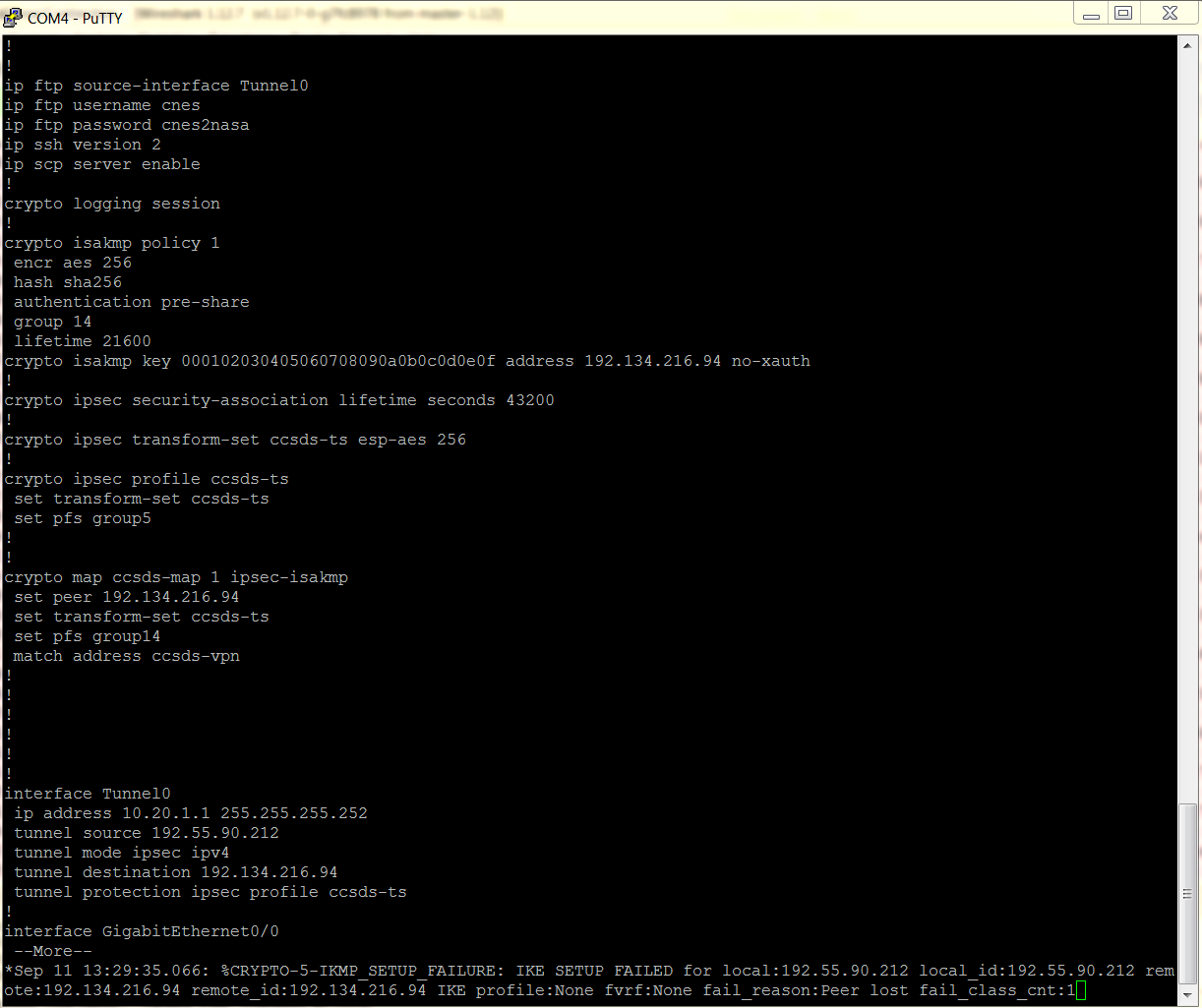
Table 5.1 is the summary of the Certificates tests performed and results.

## Certificate Validation test#1

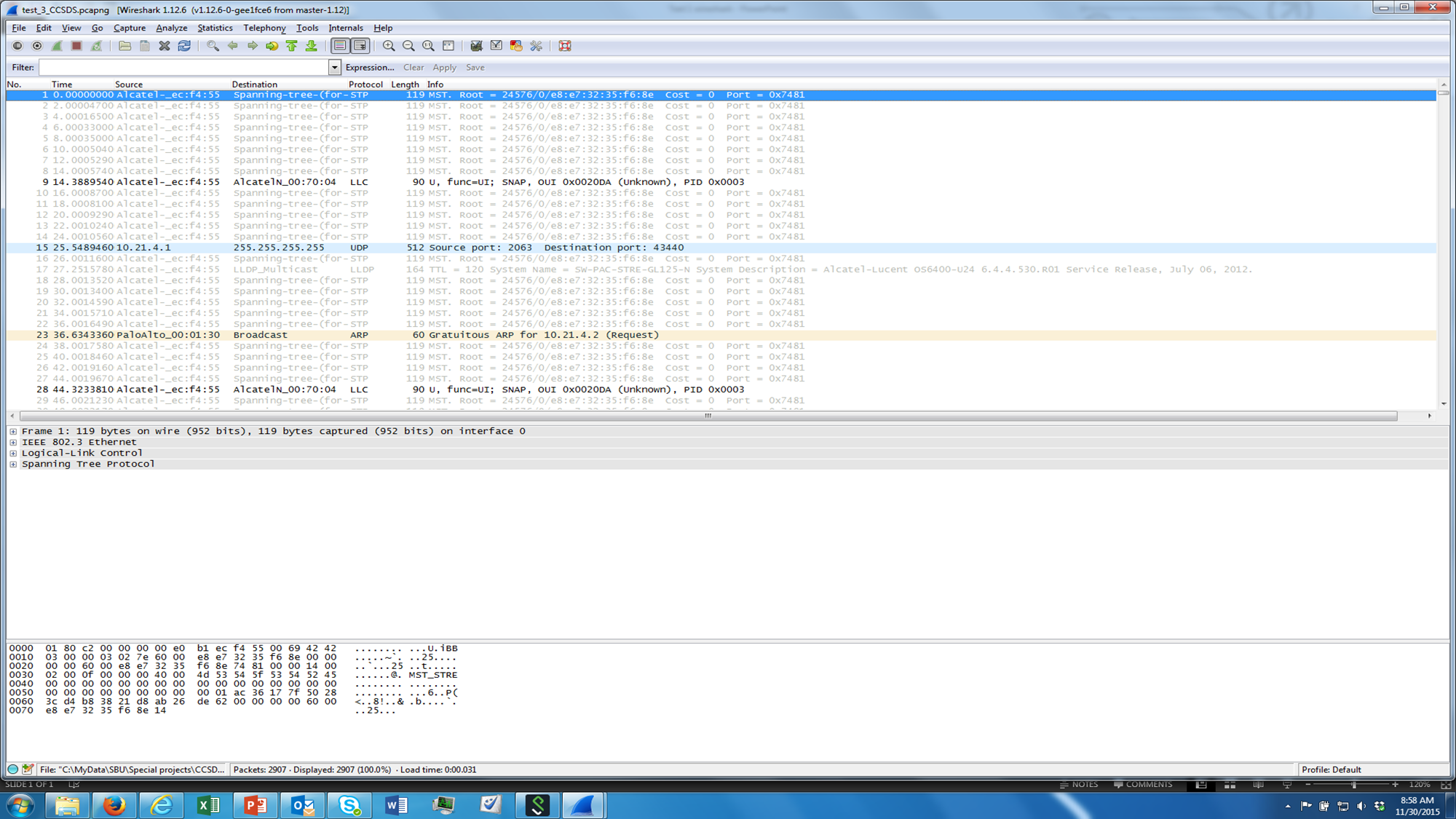
The following are the log validating the tests conducted.

|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Credentials |
| 3. | Test Case: | Read CNES Certificate |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: |  |
| 9. | Results (Pass, Partial Pass, Fail): |  |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: | Read Cert then Install Certificate |

Example test data:



CNES: test data example



## Certificate Validation test#2

The following are the log validating the tests conducted.

|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Credentials |
| 3. | Test Case: | Read NASA Certificate |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: |  |
| 9. | Results (Pass, Partial Pass, Fail): |  |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: | Read Cert then Install Certificate |

## Certificate Validation test#3

The following are the log validating the tests conducted.

|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Credentials |
| 3. | Test Case: | Read NASA encrypted e-mail at CNES |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: |  |
| 9. | Results (Pass, Partial Pass, Fail): |  |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: |  |

## Certificate Validation test#4

The following are the log validating the tests conducted.

|  |  |  |
| --- | --- | --- |
| 1. | Test Date: |  |
| 2. | Program under test: | Credentials |
| 3. | Test Case: | Read CNES encrypted e-mail at NASA |
| 4. | Agencies Participating in this Test Case: | Centre National d'Etudes Spatiales (CNES) & NASA Glenn Research Center |
| 5. | CNES Point of Contact: | Julien Airaud |
| 6. | CNES Test Engineer: | David Jean-Marie, Magnin Pierre |
| 7. | NASA Point of Contact: | Charles Sheehe |
| 8. | NASA Test Engineer: |  |
| 9. | Results (Pass, Partial Pass, Fail): |  |
| 10. | Variances from Expected Result: |  |
| 11. | Comments: |  |

# OBSERVATIONS

Place Observations about the process and the Blue Book and any recommended changes.