



ATIS-0800014

ATIS Standard on -

**SECURE DOWNLOAD AND MESSAGING
INTEROPERABILITY SPECIFICATION**



The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from over 300 communications companies are active in ATIS' 22 industry committees and its Incubator Solutions Program.

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

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.
--

ATIS-0800014, *Secure Download and Messaging Interoperability Specification*

Is an American National Standard developed by the **IPTV Security Solutions (ISS)** Committee under the **ATIS IPTV Interoperability Forum (IIF)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2008 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org/> >.

Printed in the United States of America.

SECURE DOWNLOAD AND MESSAGING INTEROPERABILITY SPECIFICATION

Secretariat

Alliance for Telecommunications Industry Solutions

Approved March 2008

Abstract

This document is one of a series of documents that specify the IPTV Security Solution (ISS). This document specifies the IPTV Security Solution/Authentication (ISS/A), which is used to authenticate downloads and messages to IPTV receiving devices. For further information, please refer to companion documents *IPTV Security Solution/Certificate (ISS/C)* [4] and *IPTV Security Solution/Root (ISS/R)* [2]. In the future, this document is expected to include the IPTV Security Solution/Encryption (ISS/E), which would be used to encrypt downloads and messages.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The IPTV Interoperability Forum (IIF) develops requirements, standards, and specifications that will determine the industry's end-to-end solution for Internet Protocol Television (IPTV).

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, IIF Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

The IPTV Security Solutions (ISS) Committee was responsible for the development of this document, with the leadership of the following people:

D. O'Callaghan, IIF Chair
R. Brand, IIF Vice Chair
J. Carr, ISS Committee Co-Chair
T. Wasilewski, ISS Committee Co-Chair
H. Hayes, Technical Editor
C.A. Underkoffler, ATIS Chief Editor
A. Blasgen, IIF Committee Administrator

CONTRIBUTORS

Cristina Serban, AT&T
D'Andre Pritchett, Irdeto
James Van Loo, Microsoft
Madjid Nakhjiri, Motorola
Sasha Medvinsky, Motorola
Petr Peterka, Motorola
Robin Wilson, Nagravision
Edmond Shapiro, NDS
Hasler Hayes, Nortel
Richard Brand, Nortel
Tony Wasilewski, Scientific-Atlanta, a Cisco Company
Mark Murray, Scientific-Atlanta, a Cisco Company
Jeff Carr, Sony
Dan O'Callaghan, Verizon
Scott Hatala, Widevine

TABLE OF CONTENTS

1 OBJECTIVES	1
2 NORMATIVE REFERENCES	1
3 ACRONYMS, & ABBREVIATIONS	2
4 OVERVIEW	2
4.1 SECURE DOWNLOAD	5
4.2 AUTHENTICATED MESSAGING	5
4.3 SECURE ENVIRONMENT OF THE IPTV RECEIVING DEVICE.....	5
4.3.1 <i>Native Security Solution (NSS)</i>	5
4.3.2 <i>ISS Security Profiles</i>	6
5 ANALYSIS FOR INTEROPERABILITY	6
5.1 AUTHENTICATION USE CASES	6
5.1.1 <i>DRM Code Download</i>	6
5.1.2 <i>Middleware and Application Download</i>	7
5.1.3 <i>Messaging and Operational Data</i>	7
5.2 ARCHITECTURAL DECOMPOSITION.....	7
5.2.1 <i>Architectural Context of Secure Persistent and Non-Persistent Data</i>	7
5.2.2 <i>Establishing Trust for Secure Persistent and Non-Persistent Data</i>	7
5.2.3 <i>IPTV Security Solution/Authentication (ISS/A)</i>	8
5.2.4 <i>Native Security Solution (NSS)</i>	8
5.2.5 <i>ISS Security Profiles</i>	9
6 DESIGN FOR INTEROPERABILITY	9
6.1 ISS/A FORMAT SPECIFICATION.....	9
6.1.1 <i>ISS/A Signature and Signed Content Specification</i>	9
6.1.2 <i>ISS/A Signed Data Specification</i>	10
6.2 ISS PROFILES	12
6.2.1 <i>Native Security Solution Chain-of-Trust</i>	13
6.2.2 <i>ISS/A Execution Environment</i>	14
6.2.3 <i>Definition of ISS Security Profiles</i>	14
6.3 ISS/A PROCESSING SPECIFICATION.....	14
6.3.1 <i>ISS/A Signing Process</i>	15
6.3.2 <i>ISS/A Signature Authentication Process</i>	15
7 REQUIREMENTS TO SPECIFICATION MAPPING	16

TABLE OF FIGURES

FIGURE 1: BASIC DRM COMPONENTS BLOCK DIAGRAM	4
FIGURE 2: ISS/A SIGNING PROCESS	5
FIGURE 3: ISS SECURITY PROFILES	13

TABLE OF TABLES

TABLE 1: ISS/A SIGNATURE AND SIGNED CONTENT SPECIFICATION	10
TABLE 2: ISS/A SIGNED DATA SPECIFICATION	11
TABLE 3: ISS SECURITY PROFILES	12

ATIS Standard for Telecommunications –

Secure Download and Messaging Interoperability Specification

1 OBJECTIVES

This Secure Download and Messaging Interoperability Specification is designed to meet the following objectives:

1. To focus on Interoperability issues only.
2. To provide a method to achieve the secure installation of the downloaded Digital Rights Management (DRM) operating code to the IPTV Receiving Device.
3. To provide a secure environment within the IPTV Receiving Device to support secure boot-loading and secure installs and updates of middleware and applications for the IPTV Receiving Device.
4. To provide a method to securely transmit and receive messages, for example to address requirements for secure Emergency Alert System (EAS) messages (Note: This version of the specification will only address the authentication aspects of secure download and messaging.)

NOTE - Service content (e.g., video and audio) authentication is not within the scope of this document and is not an expected functionality of the IPTV Security Solution.

2 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

- [1] ATIS-0800009, *Remote Management of Devices in the Consumer Domain for IPTV Services*, March 2008.¹
- [2] ATIS-0800015, *Certificate Trust Management Hierarchy Interoperability Specification*, not yet published.¹
- [3] IETF RFC 3852, R. Housley, *Cryptographic Message Syntax (CMS)*, July 2004.²
- [4] ATIS-0800016, *Standard PKI Certificate Format Interoperability Specification*, not yet published.¹
- [5] Federal Information Processing Standard (FIPS) 180-2, *Specifications for the SECURE HASH STANDARD*, August 2002.³

¹ This document is/will be available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. < <http://www.atis.org> >

² This document is available from the Internet Engineering Task Force (IETF). < <http://www.ietf.org> >

³ This document is available from the National Institute of Standards and Technology Computer Security Resource Center. < <http://csrc.nist.gov/publications/PubsFIPS.html> >

[6] ANSI X9.31, ANSI/X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry*.⁴

[7] ATIS-0800001.v002, *IPTV DRM Interoperability Requirements (Version 2)*, April 2007.⁵

3 ACRONYMS, & ABBREVIATIONS

ANSI	American National Standards Institute
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certificate Authority
CVC	Code Verification Certificate
DRM	Digital Rights Management
EAS	Emergency Alert System
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
IIF	IPTV Interoperability Forum
IP	Internet Protocol
ISS	IPTV Security Solution
ISS/A	IPTV Security Solution/ Authentication
ISS/C	IPTV Security Solution/Certificate
ISS/E	IPTV Security Solution/Encryption
ISS/R	IPTV Security Solution/Root
ITF	IPTV Terminal Function
NSS	Native Security Solution
PKCS	Public Key Cryptography Standards
STB	Set-Top Box
VOD	Video On Demand

4 OVERVIEW

The following components are involved in achieving interoperability in the IPTV Security Solution (ISS):

1. Server-Side DRM System.
2. IPTV Receiving Device DRM Component.
3. Broadcast Content Server.
4. Video on Demand (VOD) Repository.
5. VOD Server (including all types of content; e.g., video, games, music).
6. Server-Side Middleware (Subscriber/Service/Asset Management System).

⁴ This document is available from the American National Standards Institute. < <http://www.ansi.org> >

⁵ This document is available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. < <http://www.atis.org> >

7. IPTV Receiving Device (e.g., set-top box).
8. IPTV Receiving Device Software.

However, this document shall specify only the authentication functionality and authentication methodology used for securing persistent and non-persistent data for the IPTV Receiving Device.

Data is *non-persistent* when it is used only at reception time. Data is *persistent* when it is retained after reception time.

Typical examples of persistent data that may require authentication include:

- ◆ Secure download of executable software.
- ◆ Secure download of DRM code.
- ◆ Secure delivery of operational data (e.g., configuration files).
- ◆ Updates to the certificate hierarchy.

Typical examples of non-persistent data handling that may require authentication include:

- ◆ Secure delivery of EAS messages.
- ◆ Secure delivery of operational data (e.g., one-time commands).
- ◆ Secure end-to-end communications.

Figure 1 illustrates the basic components involved in the IPTV Security Solution and DRM interoperability. This specification defines an IPTV Security Solution/Authentication (ISS/A) function. The ISS/A specified in this document represents the authentication functionality necessary to enable secure download and reception of secure messages. The ISS/A may be implemented in some of the server-side elements of Figure 1 or it may be implemented in a server-side element not shown in Figure 1. On the client side, the ISS/A is implemented in the IPTV Receiving Device.

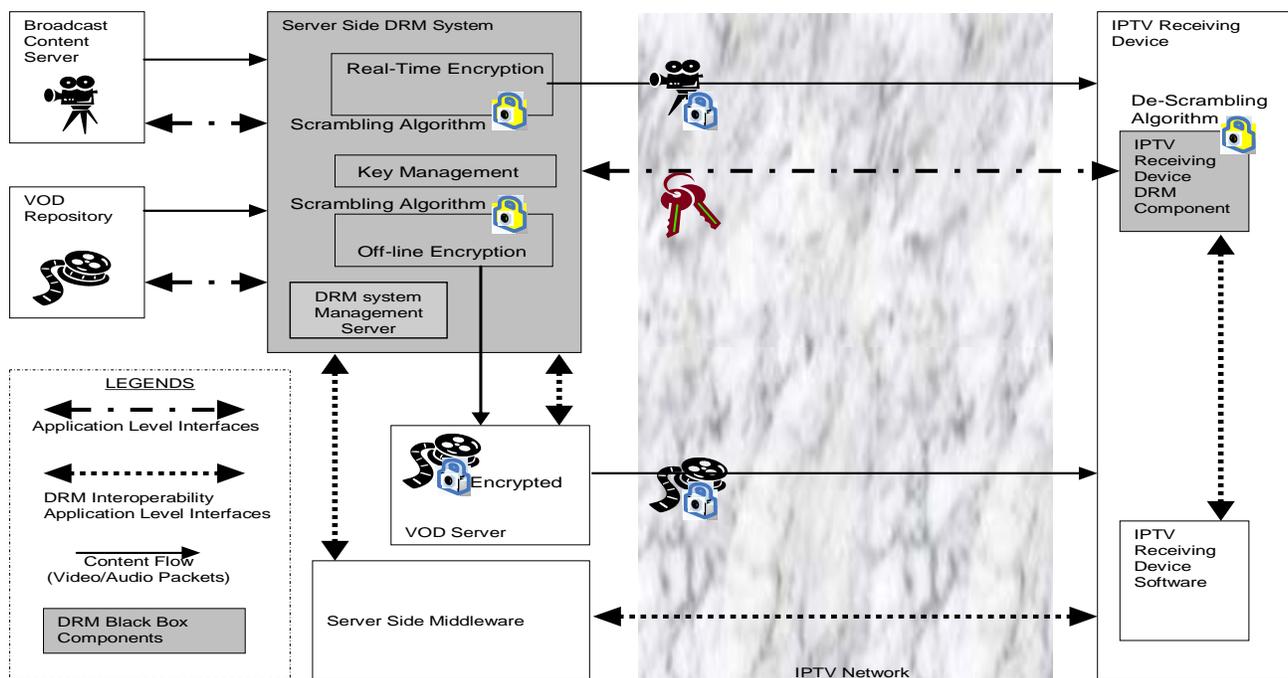


Figure 1: Basic DRM Components Block Diagram

Figure 2 shows the ISS/A within the context of the IPTV Security Solution and outlines the ISS/A process, using the signing of a software image as an example. An original software image is signed using a trusted key from a certificate that is specified in a trust management hierarchy associated with the ISS/A to create a *signed image*. The signed image is sent from a system server across the network to an IPTV Receiving Device using transport protocols found in ATIS-0800009 [1]. In the device, the ISS/A operates within the IPTV Receiving Device’s Native Security Solution (that is, its inherent hardware and software security capability) to validate the signature. Validating the signature authenticates the source of the image and verifies that the image is the original software image (verified software image).

NOTE - The treatment of content, such as messages and files, is comparable to the example of Figure 2 regardless of how they are transported in the IPTV system.

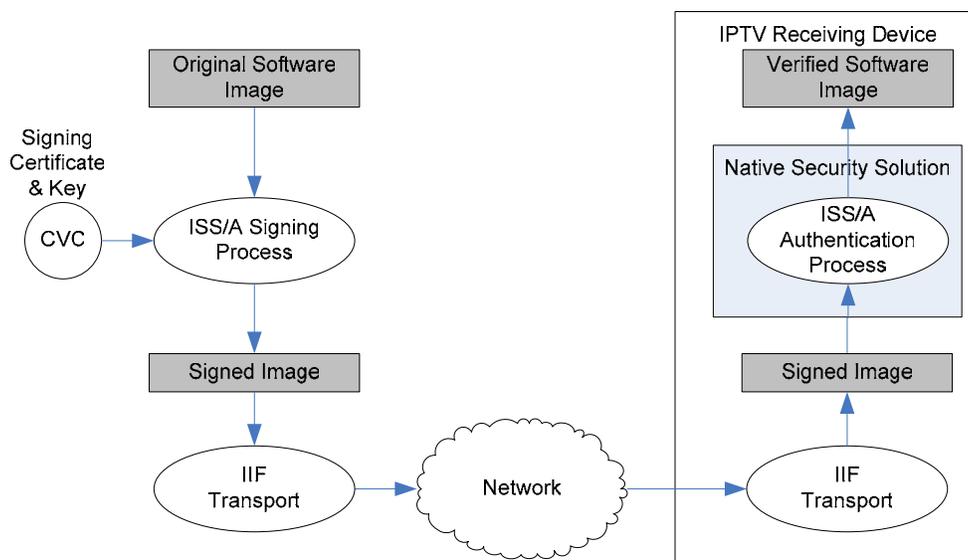


Figure 2: ISS/A Signing Process

The use of the ISS/A within the IPTV Security Solution (ISS) is motivated by the following: *secure download, authenticated messaging, and the secure environment of the IPTV Receiving Device.*

4.1 Secure Download

The operator wants the capability to securely download various executable software images into an IPTV Receiving Device. This leads to the need to ensure the authentication and integrity of software images downloaded into the IPTV Receiving Device. Note that video, audio, and data service content are not executable software images for the purposes of this specification.

4.2 Authenticated Messaging

The requirement to verify that system messages are received unmodified from legitimate sources leads to the need to ensure the authentication and integrity of the content and source of system messages. Note that the Emergency Alert System message, which could include text and audio portions, can be secured by mechanisms in this specification.

4.3 Secure Environment of the IPTV Receiving Device

To characterize the security environment of the IPTV Receiving Device, this document defines the concepts of the *Native Security Solution (NSS)* and the *ISS Security Profile*.

4.3.1 Native Security Solution (NSS)

The NSS is comprised of the hardware and software present at manufacturing time that is designed to secure the execution environment of a manufacturer’s IPTV Receiving Device. Because IPTV Receiving Devices will be designed and manufactured by different device manufacturers for a variety of different applications, the security capabilities afforded to an IPTV Receiving Device by its NSS can vary.

This specification expects the ISS/A to be incorporated into the NSS. Therefore, because the security capabilities of the NSS implementation can vary, the ISS/A must function in a manner that is independent of the specific implementation.

There are two methods in which the ISS/A may be incorporated into the NSS of an IPTV Receiving Device. They are:

1. Incorporated at the time of the IPTV Receiving Device's manufacture.
2. Downloaded and authenticated using the capabilities of the NSS.

4.3.2 ISS Security Profiles

The ISS/A is vulnerable to subversion or imitation if the execution environment of the IPTV Receiving device is not sufficiently secure. This document introduces the concept of an ISS Security Profile as a means to classify security characteristics of a specific implementation of an IPTV Receiving Device. In particular, these profiles define the characteristics of the execution environment in which the NSS and hence the ISS/A operate.

5 ANALYSIS FOR INTEROPERABILITY

5.1 Authentication Use Cases

The following sections define use cases for:

- ◆ Downloading DRM code to the IPTV Receiving Device.
- ◆ Downloading middleware and application software to the IPTV Receiving Device.
- ◆ Securing messages and operational data sent to the IPTV Receiving Device.

The secure download and messaging security functions will operate in a manner independent of the specific download or message transport mechanism. This specification provides defined mechanisms for assuring the authenticity and integrity of downloads and messages. A later version of this specification will support confidentiality through the addition of an encryption function to be called the *IPTV Security Solution/Encryption (ISS/E)*.

5.1.1 DRM Code Download

The following use cases are provided to assist in the analysis of the DRM operating code downloaded into the IPTV Receiving Device. The purpose of the analysis is to identify functionality necessary to ensure that the secure download of the IPTV Receiving Device DRM code is interoperable with the overall IPTV Security Solution.

- ◆ The DRM code received by the IPTV Receiving Device is received from an approved sender.
- ◆ The DRM code received by the IPTV Receiving Device is unaltered from that sent by the approved sender.
- ◆ The DRM code received by the IPTV Receiving Device is communicated in a manner which preserves integrity and (in a later revision of this specification) confidentiality.

5.1.2 Middleware and Application Download

The following use cases are provided to assist in the analysis of the Middleware and Application code downloaded into the IPTV Receiving Device. The purpose of the analysis is to identify functionality necessary to ensure that the secure download of the IPTV Receiving Device Middleware and Applications is interoperable with the overall IPTV Security Solution.

- ◆ The Middleware and/or Applications received by the IPTV Receiving Device are received from an approved sender.
- ◆ The Middleware and/or Applications received by the IPTV Receiving Device are unaltered from that sent by the approved sender.
- ◆ The Middleware and/or Applications received by the IPTV Receiving Device are communicated in a manner which preserves integrity and (in a later revision of this specification) confidentiality.

5.1.3 Messaging and Operational Data

The following use cases are provided to assist in the analysis of the transfer of Messages and Operational Data into the IPTV Receiving Device. The purpose of the analysis is to identify functionality necessary to ensure that the secure transfer of the IPTV Receiving Device Messages and Operational Data is interoperable with the overall IPTV Security Solution.

- ◆ The Messages and/or Operational Data received by the IPTV Receiving Device are received from an approved sender.
- ◆ The Messages and/or Operational Data received by the IPTV Receiving Device are unaltered from those sent by the approved sender.
- ◆ The Messages and/or Operational Data received by the IPTV Receiving Device are communicated in a manner which preserves integrity and (in a later revision of this specification) confidentiality.

5.2 Architectural Decomposition

5.2.1 Architectural Context of Secure Persistent and Non-Persistent Data

The IPTV architecture specified by the IIF distinguishes between the mechanisms and protocol stack that transport persistent data (e.g., code downloads, configuration files) or non-persistent data (e.g., EAS messages). The mechanisms defined in this specification ensure the integrity, authenticity, and (in a later revision of this specification) confidentiality of these data types.

5.2.2 Establishing Trust for Secure Persistent and Non-Persistent Data

One prerequisite for secure communications is the establishment of trust between an approved sender and the IPTV Receiving Device. This trust is based upon:

- ◆ Standard Public Key Infrastructure (PKI) mechanisms rooted with the IPTV Security Solution/Root (ISS/R) certificate, ATIS-0800015 [2].
- ◆ A PKI Trust Management Hierarchy. The detailed specification for the Trust Management Hierarchy is addressed in ATIS-0800015 [2].
- ◆ A suitable execution environment.

5.2.3 IPTV Security Solution/Authentication (ISS/A)

The ISS/A specified herein uses data structures and semantic contracts to define its operation and therefore is not specified as a component with application programming interfaces. In addition, this specification is based on the existence of a NSS on the IPTV Receiving Device that secures the execution environment of the ISS/A.

5.2.3.1 Using the ISS/A for Persistent Data

By verifying a digital signature and certificate linked back to the Trust Management Hierarchy:

- ◆ The ISS/A will check the integrity and authenticity of the received persistent data.
- ◆ The ISS/A will check the integrity and authenticity of persistent data in the form of executable software images when they have been stored in non-secured storage.
- ◆ The ISS/A will check the integrity and authenticity of persistent data that affects the context and operation of executable software images when they have been stored in non-secured storage.

5.2.3.2 Using the ISS/A for Non-Persistent Data

By verifying a digital signature and certificate linked back to the Trust Management Hierarchy, the ISS/A will check the integrity and authenticity of received non-persistent messages.

5.2.3.3 ISS/A Security Method

The preferred approach to protect the integrity and prove the authenticity of a software image or message is to apply a digital signature to the image or message. The digitally signed software image or message will be validated before execution of the software or processing of the message. For interoperability purposes, it is necessary to have both a standardized data format and standardized semantics for the digital signature.

Secure download objects and messages will be digitally signed using standard public key infrastructure technology. Data will be signed with a trusted private key. The digital signature will be validated using a corresponding trusted public key. Trust of the public key is established by validating its authenticity back to a root trust authority. The Trust Management Hierarchy is defined in ATIS-0800015 [2].

5.2.4 Native Security Solution (NSS)

The NSS establishes the security environment in which the ISS/A exists and executes. Examples of NSS functionality are:

- ◆ The NSS may provide functionality that enables authentication and integrity checking of the ISS/A at any time, including at ISS/A download or boot time of the IPTV Receiving Device.
- ◆ The NSS working with the ISS/A must be sufficiently secure to mitigate the threat risks to the IPTV Receiving Device. The relevant threat risks will be addressed in a future ATIS specification dealing with robustness rules. The provisioning of the ISS/R to the IPTV Receiving Device may be performed by the NSS.

NOTE - The provisioning of the ISS/A and the ISS/R into the IPTV Receiving Device may be performed at the time of manufacture. In this case, use of a NSS authentication function is optional.

5.2.5 ISS Security Profiles

The overall security characteristics of the IPTV Receiving Device are dependent on the NSS implementation in conjunction with the ISS/A. In this specification, the concept of an ISS Security Profile is introduced as a means of classifying the security characteristics of a specific implementation of an IPTV Receiving Device. These profiles:

- ◆ Support commercial decisions regarding what content will be made available to the IPTV Receiving Device.
- ◆ Give device manufacturers flexibility in the implementation of the IPTV Security Solution.
- ◆ Provide operators with a basis to specify security requirements for IPTV Receiving Devices.

As mentioned previously, the ISS/A is authenticated by the NSS before it is allowed to execute.

The use cases previously discussed in this document identify the need for the chain-of-trust to be used by the ISS/A to, for example, authenticate downloaded executable software and messages. It is also the intent of this document to define the best security environment possible on specific classes of implementation platforms. To this end, the capabilities of the NSS must be considered.

6 DESIGN FOR INTEROPERABILITY

This section defines the ISS/A standard digital signature format and processing requirements. ISS-compliant secure downloads and secure messages **shall** use the following mechanisms. This specification does not preclude the IPTV Receiving Device from using other mechanisms for authentication of messages and images. However, an ATIS IIF-compliant IPTV Receiving Device must include the ISS/A authentication mechanism.

6.1 ISS/A FORMAT SPECIFICATION

The signature and data to be processed by the ISS/A **shall** be formatted in a PKCS#7 compatible structure compliant to RFC 3852 [3]. All signature fields **shall** comply with RFC-3852 definitions with the additional restrictions noted in the text immediately following Table 1 and Table 2. If the description of a field is blank, it implies conformance to RFC 3852 with no further modifications.

6.1.1 ISS/A Signature and Signed Content Specification

The structure of the following table **shall** be used to form the ISS/A signature and signed content structure.

Table 1: ISS/A Signature and Signed Content Specification

Field	Description
Signature {	
ContentInfo	{ 1.2.840.113549.1.9.16.1.6 }
ContentType	SignedData { 1.2.840.113549.1.7.2 }
SignedData ()	See Table 2
}end Signature	
SignedContent {	
Content ()	Sequence of Octets for Software image or message.
}end SignedContent	

ISS/A constraints to RFC 3852 [3] practice are:

The ContentType **shall** always be SignedData.

The SignedContent **shall** be external to the Signature and **shall** be appended to the Signature as shown in Table 1. The Content () appended to the Signature is the software image or message that is being digitally signed. The ISS/A makes no assumptions about the Content () .

6.1.2 ISS/A Signed Data Specification

The structure of the following table **shall** be used to form the SignedData() field within the ISS/A Digital Signature structure.

Table 2: ISS/A Signed Data Specification

RFC3852 Field	Description
SignedData {	
version	
digestAlgorithms	
encapContentInfo	
ContentType	Data { 1.2.840.113549.1.7.1 } The Content () is appended to the ISS/A Digital Signature per "External Signature" method defined in RFC-3852.
certificates {	
ContentSignerCVC	Required
CVC CA	Optional
} end certificates	
crls	shall NOT be used in this structure
signerInfo {	
version	version=1
sid	
issuerName	Refer to ATIS-0800015
serialNumber	Refer to ATIS-0800015
digestAlgorithm	SHA-1 { 1.3.14.3.2.26 } shall be supported, SHA-256 { 2.16.840.1.101.3.4.2.1 } SHOULD be supported, and others not precluded
signedAttrs	
contentType	{ 1.2.840.113549.1.9.3 } (required) (always Data { 1.2.840.113549.1.7.1 })
messageDigest	{ 1.2.840.113549.1.9.4 } (required)
signingTime	{ 1.2.840.113549.1.9.5 } (optional) UTC Time (GMT), YMMDDHHMMSSZ
signatureAlgorithm	SHA-1 with RSA Encryption { 1.2.840.113549.1.1.5 } shall be supported, SHA-256 with RSA Encryption { 1.2.840.113549.1.1.11 } SHOULD be supported, and others not precluded
signature	
unsignedAttrs	(optional)
} end signerInfo	
}end SignedData	

ISS/A constraints to RFC 3852 [3] practice are:

- ◆ encapContentInfo is always Data { 1.2.840.113549.1.7.1 }. Image/file/message data is not encapsulated in the SignedData(), but instead follows the "external signature" method described in RFC 3852 [3] Section 5.2.

ATIS-0800014

- ◆ certificates follow the format specified in ATIS-0800016 [4]. A signer(s) certificate appropriate to the content **shall** always be included. Additional Certificate Authority (CA) certificates may be included as necessary to complete the trust-linkage of the signer(s) certificates back to the ISS/R.
- ◆ `crls` (certificate revocation lists) are not provided in the ISS/A `SignedData()` structure. Certificate revocation lists are delivered to the IPTV Receiving Device by methods outlined in ATIS-0800015 [2].
- ◆ `sid` in the `signerInfo` **shall** be of the `issuerAndSerialNumber` form as identified by `version=1`.
- ◆ `issuerName` and `serialNumber` are of the form specified in ATIS-0800016 [4]. Note that the OU field in the `issuerName` identifies the intended purpose for which the certificate was issued (e.g., OU=ATIS code signing).
- ◆ `digestAlgorithm`, see Table 2, Federal Information Processing Standard (FIPS) 180-2 [5].
- ◆ `signatureAlgorithm`, see Table 2, ANSI X9.31 [6].

NOTE - The IIF recognizes that, according to the US federal government, SHA-1 has a limited lifetime of secure usage. A future revision of this specification will address this point. For the present, implementers are strongly encouraged to migrate to SHA-256 as soon as possible.

6.2 ISS Profiles

The following security profiles are defined:

Table 3: ISS Security Profiles

Name	Chain-of-trust	Execution Environment
ISS Profile 0	None	Non-Secured
ISS Profile 1	Indirect	Non-Secured
ISS Profile 2	Direct	Non-Secured
ISS Profile 3	Indirect	Secured
ISS Profile 4	Direct	Secured

The figure below illustrates these profiles. The definitions of the profile attributes are given in the following subsections.

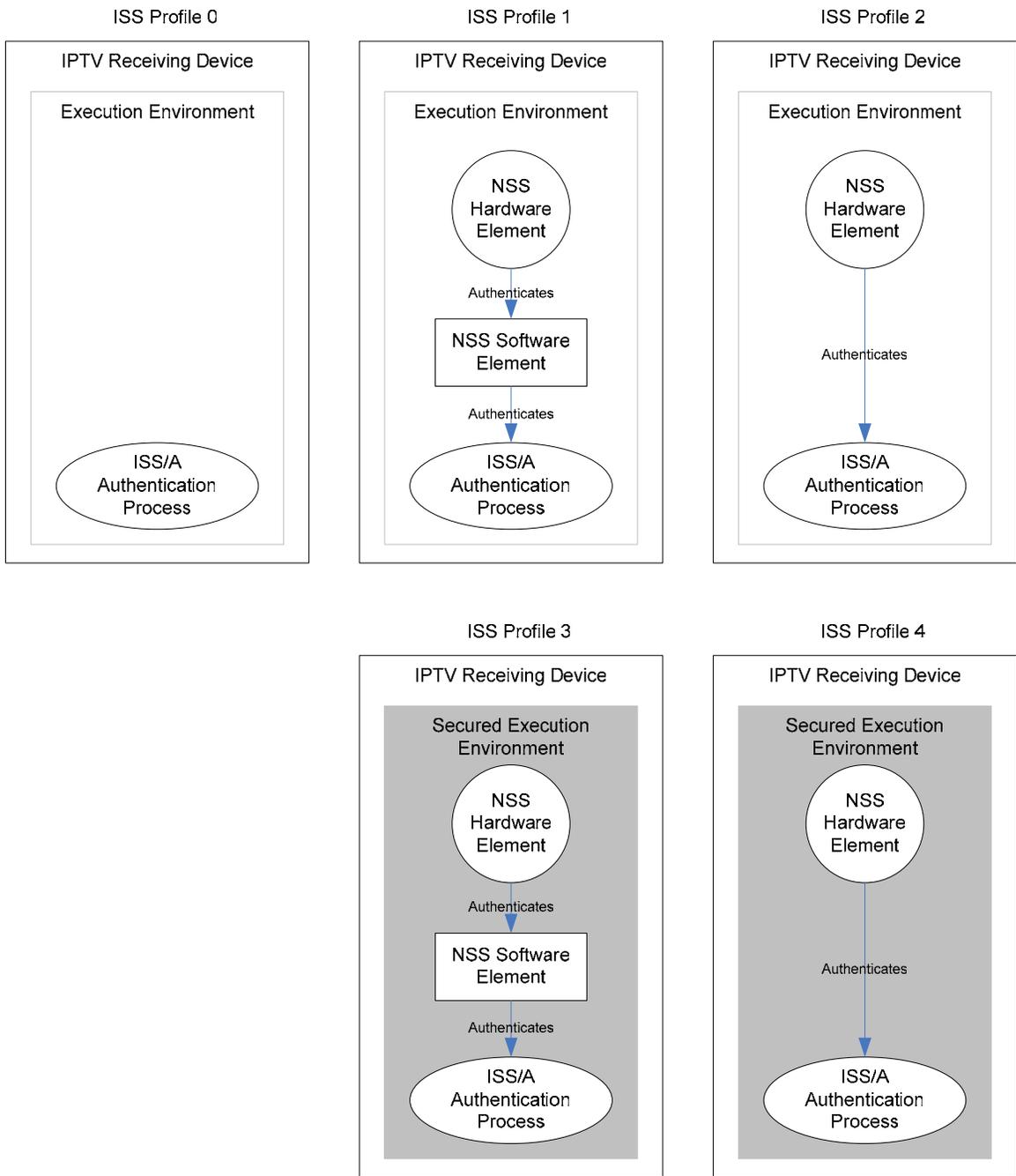


Figure 3: ISS Security Profiles

6.2.1 Native Security Solution Chain-of-Trust

The NSS chain-of-trust refers to the method by which the implementation of the ISS/A is verified before it is allowed to execute.

- ◆ “None” means that the ISS/A is initiated without any authentication of its code or included certificates, if any.
- ◆ “Indirect” means that the ISS/A is authenticated and initiated by trusted software on the IPTV Receiving Device. That trusted software is authenticated by the NSS hardware element.
- ◆ “Direct” means that the ISS/A is authenticated and initiated by the NSS hardware element.

6.2.2 ISS/A Execution Environment

The ISS/A Execution Environment can be differentiated into two contexts.

- ◆ A “secured” execution context is one that conforms to a future ATIS specification dealing with robustness rules.
- ◆ A “non-secured” execution context is one that does not conform to a future ATIS specification dealing with robustness rules.

6.2.3 Definition of ISS Security Profiles

The following defines ISS profiles:

- ◆ *ISS profile 0* is defined as:
 - No authentication and no integrity check (i.e., there is no chain of trust and the execution environment is non-secured).
- ◆ *ISS profile 1* is defined as:
 - Authentication and integrity are verified by software on the IPTV Receiving Device (i.e., an indirect chain of trust).
 - An execution environment that is non-secured.
- ◆ *ISS profile 2* is defined as:
 - Authentication and integrity are verified by hardware on the IPTV Receiving Device (i.e., a direct chain-of-trust).
 - An execution environment that is non-secured.
- ◆ *ISS profile 3* is defined as:
 - Authentication and integrity are verified by software on the IPTV Receiving Device (i.e., an indirect chain-of-trust).
 - A secured execution environment.
- ◆ *ISS profile 4* is defined as:
 - Authentication and integrity are verified by hardware on the IPTV Receiving Device (i.e., a direct chain-of-trust).
 - A secured execution environment.

6.2.4 Certification of ISS Security Profiles

The ISS Security Profile associated with a device is indicated within an extension field of the device’s ISS/C (see ATIS-0800016 [4]).

6.3 ISS/A Processing Specification

The ISS/A process involves two steps as highlighted in Figure 2: 1) a *signing process*; and 2) an *authentication process*.

A pair of mathematically related keys is used in the signing and authentication process. A secret private key is used at the signing time, and a freely known public key is used at authentication time.

A hash digest of the content is computed at both signing and authentication time. The hash computed at signing time is encrypted with the private key and becomes part of the digital signature. At

authentication time it is decrypted with the public key and compared to the newly computed hash. This ensures the data is unchanged since signing time and the signature was generated by the holder of the private key.

Each authorized signer is granted a certificate that contains its public key, identification information, and a digital signature signed by a higher-level trusted Certificate Authority (CA). The same authentication process used to digitally sign content data is also used to sign the certificates, linking them in a chain of trust back to a trusted root certificate (ISS/R). See ATIS-0800015 [2].

6.3.1 ISS/A Signing Process

The ISS/A signing process involves generating the digital signature header that is prefixed to the signed content. The ISS/A signer must also have a secret private key and public key certificate issued by an ATIS-authorized CA.

The steps below provide a summary of the operations performed:

1. `DigitalSignature` header fields are prepared and attributes set as described in Section 6.1.
2. A hash digest is computed that covers the `signedAttrs` and `Content()`. The hashing algorithm used is identified in the `digestAlgorithm` field.
3. The hash value is saved in the `messageDigest` field.
4. The `messageDigest` is also encrypted using the secret private key and put in the `signature` field.
5. A copy of the signers' certificate(s) is (are) placed in the `certificates` field.
6. The `DigitalSignature` header is prefixed to the `Content()` and together become the Signature and Signed Content Specification.

6.3.2 ISS/A Signature Authentication Process

The ISS/A authentication process involves checking the digital signature header and verifying the hash computed from the data is the same as the value computed at signing time. In addition, the certificate that identifies the signer must be linked back into the Trust Management Hierarchy to a trusted root certificate.

The steps below provide a summary of the operations performed:

1. `DigitalSignature` header fields are checked for proper formatting and values as specified in Section 6.1.
2. A hash digest is computed that covers the `signedAttrs` and `Content()`. The hashing algorithm used is identified in the `digestAlgorithm` field.
3. The hash value is compared to the `messageDigest` field.
4. The encrypted hash from the `signature` field is decrypted using the signers' public key found in the `certificates` field and compared to the `messageDigest`.
5. The signers' certificate(s) is (are) from the `certificates` fields is linked to into the Trust Management Hierarchy using a similar authentication process. Content signer(s) certificate(s) **shall** always be included.

The process of authenticating and rules for using a certificate in the Trust Management Hierarchy is described in more detail in ATIS-0800015 [2].

7 REQUIREMENTS TO SPECIFICATION MAPPING

This specification addresses, in whole or in part, the following requirements of ATIS-0800001.v002 [7].

IIF.DRM.General.2100-0200 - The IPTV security solution **shall** support a mechanism to allow for the authenticity of signaling messages.

IIF.DRM.General.2100-0300 - The IPTV security solution **shall** support a mechanism to allow for the integrity of signaling messages.

IIF.DRM.General.2200 - The IPTV security solution **shall** provide a secure execution environment in the IPTV Receiving Device by supporting secure boot-loading and secure installs and updates of middleware and applications for the IPTV Receiving Device DRM Component.

IIF.DRM.General.2300 - The IPTV Security Solution **shall** support secure download and install of the DRM operating code to IPTV Receiving Devices.

IIF.DRM.Operator.0600 - The IPTV security solution **shall** provide a mechanism to allow IPTV operator to securely update the parameters (e.g., configuration) of IPTV Receiving Device DRM Components.

IIF.DRM.Operator.0700 - The IPTV security solution **shall** provide a mechanism to allow the IPTV operator to securely load the IPTV Receiving Device DRM Component to the IPTV Receiving Devices.