ATIS Downloadable Security
An
IPTV Downloadable Security Report

January 2009

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 more than 350 communications companies are active in ATIS' 22 industry committees, and its Incubator Solutions Program.

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

This document is the ATIS IPTV Downloadable Security Report produced by the ATIS IP-Based Separable Security Incubator (AISP.5-ISSI). In the Report and Order FCC 00-342, the FCC acknowledged the Cable industry's request for downloadable security as an alternative to the CableCARD. This report defines the IPTV downloadable security functionality including system overview, assessments, physical implementations, and recommendations.

This document is a *work in progress* and subject to change.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Printed in the United States of America.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) incubator program serves the public through improved understanding between stakeholders. The mission of the ATIS Incubator Solutions Program #5 on IP-based Separable Security Incubator (AISP.5-ISSI) is to create two distinct solutions for IP-based separable security in the emerging IPTV market that will achieve the objectives set forth by the Federal Communications Commission in CS Docket No. 97-80.

1. An enhancement of the existing CableCARD™ specification as defined in SCTE-28 to enable IP flows that are agnostic to the network technology of the service/network provider.

   Ensure the physically separable solution is harmonized with, and backwards compatible to, the existing unidirectional CableCARD™ standard

2. A common target platform for a downloadable security functionality that eliminates the physical device mentioned above while meeting the security criteria defined in FIPS 140-2.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, AISP.5-ISSI Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

AISP.5-ISSI COMMITTEE LIST

Name	Company	Name	Company
Konstantin Livanos	Alcatel-Lucent	Madjid Nakhjiri	Motorola
Madhu Penugonda	CCAD, LLC	Robin Wilson	Nagravision
Dhawal Moghe	CableLabs	Steve White	Nagravision
Kinney Bacon	Cisco	Mark Eyer	Sony Electronics
Tony Wasilewski	Cisco	Tony Aoki	Sony Electronics, ISSI Vice Chair
Nandhu Nandhakumar	LG Electronics	Dan O'Callaghan	Verizon
Andrea Harriman	Motorola	Michael Nawrocki	Verizon, ISSI Chair
Kyle Woodward	Motorola	Robert Schafer	Verizon
Niranjan Samant	Motorola	Glenn Morten	Widevine
Sasha Medvinsky	Motorola	Jim Veres	Widevine
Tat Chan	Motorola		

The **AISP.5-ISSI** was responsible for the development of this document.

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 the validity of this claim or any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the publisher.

Table of Contents

1 Introduction 1

1.1 SCOPE 1

1.2 PURPOSE 1

2 Normative References 1

3 Downloadable Security Overview (Informative) 2

3.1 ARCHITECTURE 2

3.1.1 Downloadable Security Block Diagram 2

3.1.2 Secure Environment Reference Points 3

3.1.3 Host Reference Points 4

3.2 DOWNLOAD MANAGER 7

3.2.1 Basic Functionality 7

3.2.2 Functional Extensions 7

4 Downloadable Security Assessment 10

4.1 DOWNLOADABLE SECURITY ALTERNATIVES 10

4.2 ASSESSMENT CRITERIA 10

4.3 ASSESSMENT OF DOWNLOADABLE SECURITY ALTERNATIVES 11

4.4 RANKING OF DOWNLOADABLE SECURITY ALTERNATIVES 14

5 Downloadable Security Physical Implementations 15

5.1 A-POD-BASED DOWNLOADABLE SECURITY 15

5.2 CPCM-BASED DOWNLOADABLE SECURITY 16

6 Downloadable Security Recommendations 17

6.1 RECOMMENDED TARGET SOLUTION 17

6.2 RECOMMENDED NEXT STEPS 17

6.2.1 Form a Business Issues Focus Group 17

6.2.2 Recommended Standards Venue 17

6.2.3 Coordination with Other Industry Activities 18

6.2.4 Other Factors Impacting Acceptability 18

6.3 PROJECTED TIMELINE FOR COMPLETION OF SPECIFICATION 18

Appendix A- Acronyms 19

Table of Figures

FIGURE 1: DOWNLOADABLE SECURITY BLOCK DIAGRAM 3
FIGURE 2: A-POD-BASED DOWNLOADABLE SECURITY BLOCK DIAGRAM 15
FIGURE 3: CPCM-BASED DOWNLOADABLE SECURITY BLOCK DIAGRAM 16

Table of Tables

TABLE 1: ASSESSMENT OF DOWNLOADABLE SECURITY ALTERNATIVES 13
TABLE 2: DOWNLOADABLE SECURITY ALTERNATIVES AND CRITICAL FUNCTIONS COMPARISON 14

1 INTRODUCTION

1.1 SCOPE

This report defines the IPTV downloadable security functionality, where in the FCC Report and Order FCC 00-342 is an alternative to the CableCARD™. This report includes a system overview, assessments, physical implementations, and recommendation regarding the following downloadable security alternatives.

- Client Loaded into Untrusted Platform
- Client Loaded into a Defined Security Environment
- Client Loaded into a Qualified Security Part(s)
- Client Loaded into a Low Cost Removable Medium
- Client Loaded into a Qualified Secure Part with Secret Information in a Low Cost Removable Medium
- Secure Environment Based on a Virtual Machine Abstraction

1.2 PURPOSE

The purpose of this Downloadable Security Report is to review alternatives for downloadable security and provide a target solution. It is expected that downloadable security will accomplish the following goals:

- Provide a level of security that enables operators to securely deliver high value content
- Reduce cost through the elimination of external physical devices
- Accommodate security replacements and upgrades

2 NORMATIVE REFERENCES

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

[SYSSEC]	OC-SP-SEC-I07-061031 OpenCable System Security Specification
[TIA/EIA 568 B]	ANSI/TIA/EIA-568-B.1-2001, -B.2-2001, and -B.3-2001
[IEEE 802.3ab]	ANSI/IEEE 802.3ab-1999
[CPCM]	Digital Video Broadcasting (DVB) BlueBook A094r2 Content Protection and Copy Management
[ATIS-0800014]	Secure Download and Messaging Interoperability Specification
[ATIS-0800015]	Certificate Trust Management Interoperability Specification