



An Open Framework

Ensuring IPTV's Interoperable Content Security

Speakers

Dan O'Callaghan



Vice Chair
ATIS IPTV Interoperability Forum
Member of the Technical Staff
Verizon Communications

Tony Wasilewski



Co-Chair
ATIS IPTV Security Solutions Committee
Distinguished Engineer
Service Provider Video Technology Group
Cisco Systems



Outline

- In IPTV – Everything Needs to Be secured
- Device security is not “one size fits all”
- Open Security Framework
- The IPTV Security Solutions (ISS) Toolkit
- Integrating different CAS and DRM systems with the network



In IPTV **Everything** Needs to Be Secured!

- Its not just the content:
 - Devices and users need to be authenticated
 - Downloads and messages need to be authenticated and confidential
 - Devices need to have trusted levels of security robustness
 - Different CAS and DRM choices must integrate securely with the network



Device Security

- No single device security target anymore
- Different types of devices support different security functionality and robustness
 - some more than others
- Need a robustness abstraction that allows maximum flexibility in device design and manufacture while still characterizing intrinsic device security
- Need a classification scheme that represents the abstraction and supports content owners' desire to specify value-based content playout



Open Security Framework

- ISS does NOT define a CAS or DRM (Specific security products are considered to be black boxes)
- Framework embraces Simulcrypt principles
- ISS redefines and updates the common scrambling algorithm, can leverage Simulcrypt in the headend and defines common application interfaces both in the service provider and consumer domains
- The ISS framework uses a toolkit approach based on a Trust Management Hierarchy (PKI) with well-defined robustness rules



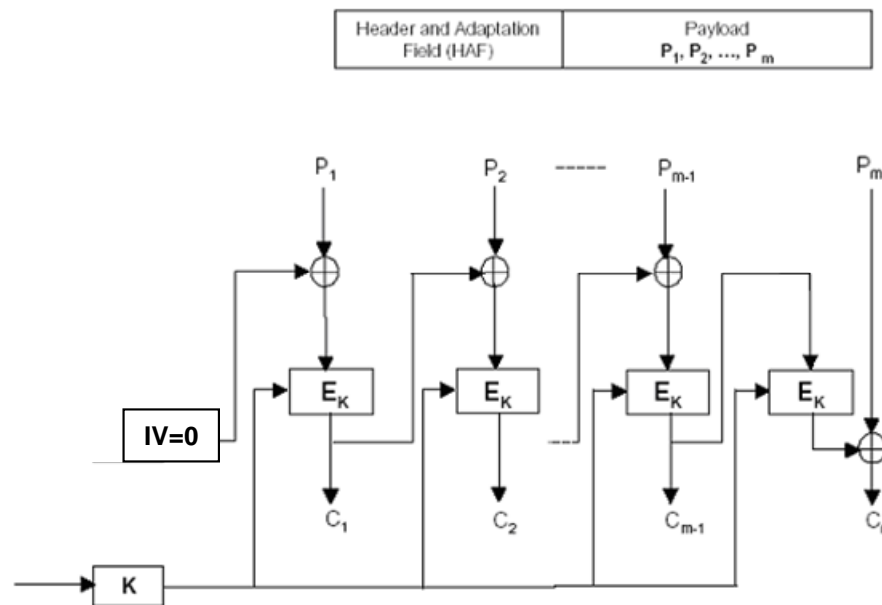
Toolkit Approach

- IPTV Security Solutions (ISS) Committee provides tools for:
 - Content Scrambling (ISS/S)
 - Authentication (ISS/A)
 - Confidentiality or Encryption (ISS/E)
 - Root Certificates (ISS/R)
 - Device Certificates (ISS/C)
 - Certificate Authority Certificates (ISS/CA)
 - Security Robustness Rules
 - Client side security APIs
 - Server side security APIs
 - DeviceID (ISS/I?)



ISS/S – IIF Default Scrambling Algorithm (IDSA)

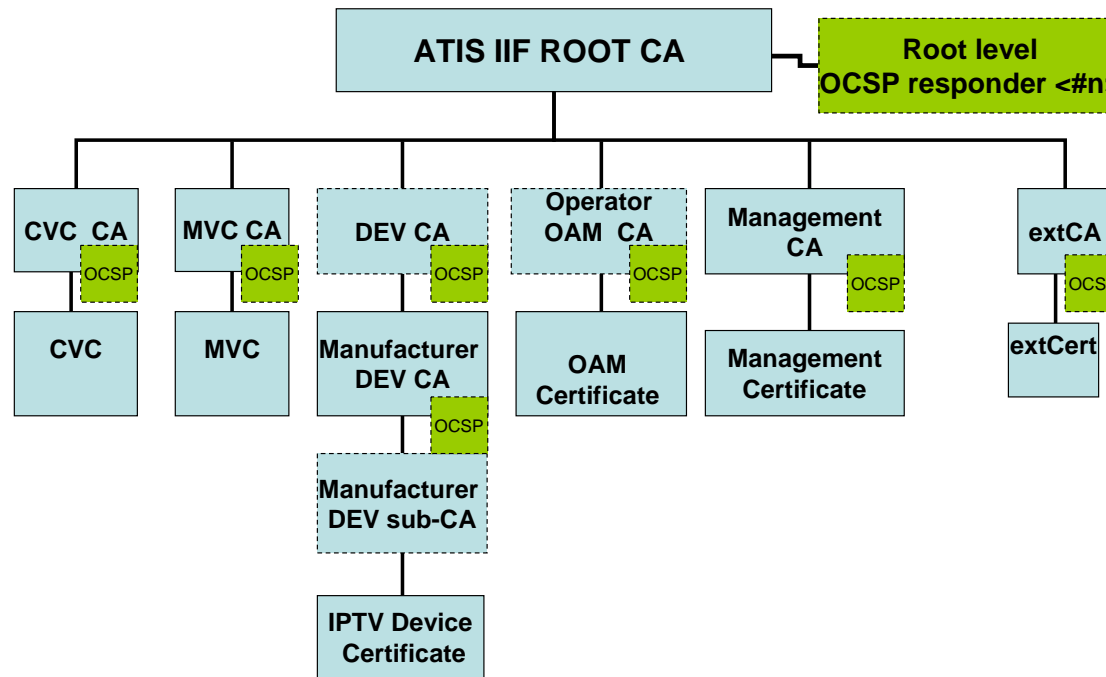
- IDSA and scrambling algorithm signaling: ATIS-0800006
- IDSA is 128-bit AES-based CBC mode block cipher
- Currently Mapped to MPEG-2 Transport only





IIF Trust Management Hierarchy

- ATIS-0800015 specifies a Trust Hierarchy that supports device, code download and message authentication based on a PKI and root of trust





Certificates

IIF Trust Hierarchy is based on ITU-T X.509 certificates as profiled in RFC 5280

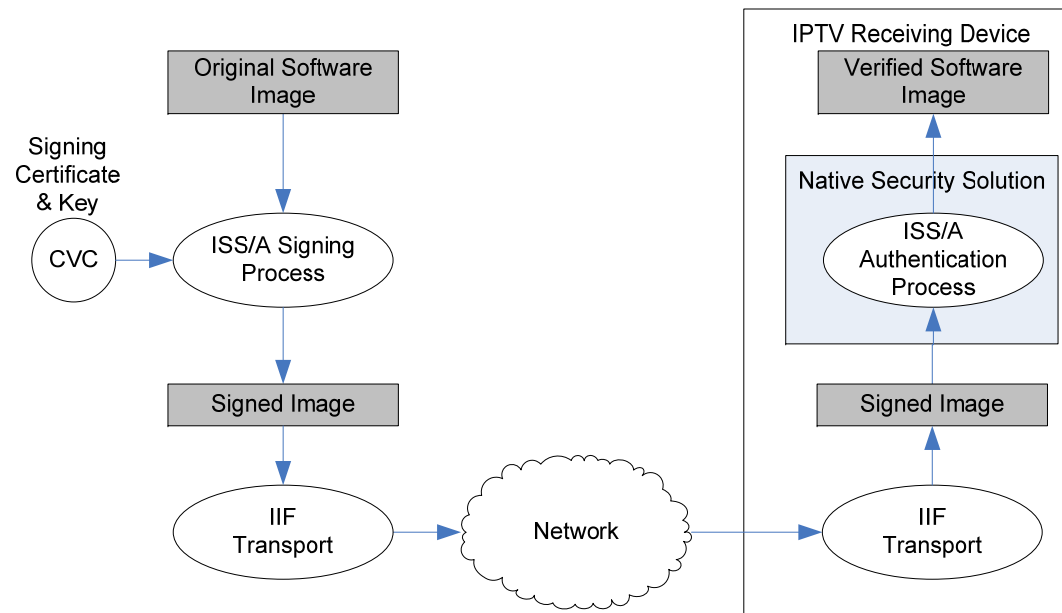
- ATIS-0800016 defines the format of three types of certificates used in the IIF Trust Hierarchy
 - ISS/R Root
 - ISS/CA Certificate Authority
 - ISS/C Leaf nodes of hierarchy
- Each certificate type has various mandatory and/or optional extensions



Device and Message Authentication – ISS/A

- ATIS-0800014.v002 specifies a general purpose approach (based on RFC 3852 with extensions) for authenticating and providing confidentiality to code downloads and service messages

**Signature
Algorithm is
SHA-256 with
RSA
Encryption**





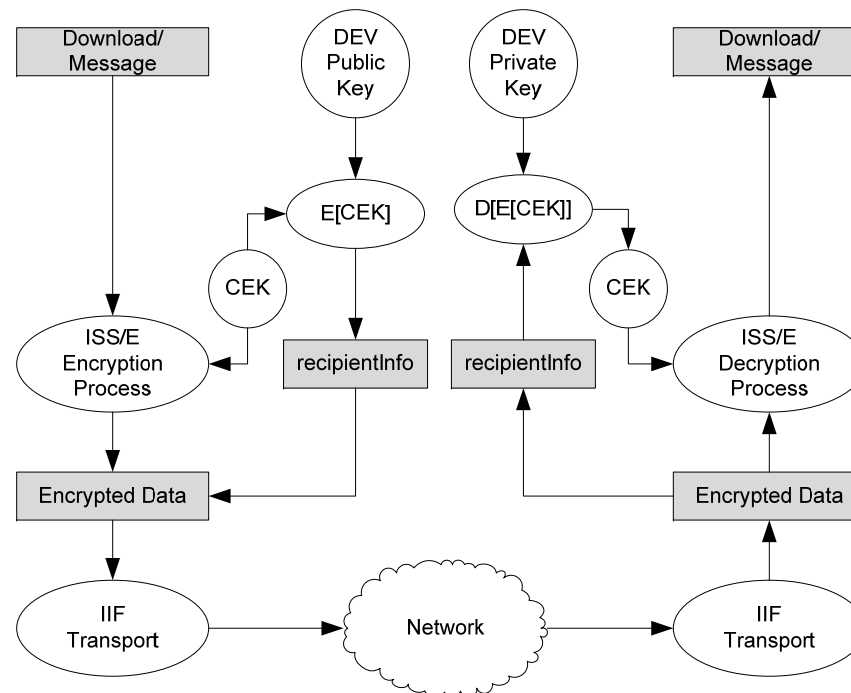
Message Confidentiality – ISS/E

- Two methods based on RFC 3852 and RFC 3560: Key Transport and Pre-provisioned Key (key transport shown)

Content Encryption Algorithm is AES-CBC 128 bits, IV=0

Key Encryption Algorithm is RSAES-OAEP

ISS/A and ISS/E can be used together on same code or message





Device Security

- ATIS-0800014.v002 defines 5 security profiles that identify:
 - whether and how the device is participating in the chain of trust
 - how secure the security client software environment is
- ATIS-0800024 defines Secure Execution Environment (SEE) levels and the robustness characteristics of these levels
 - robustness levels are related to concepts found in popular device security licensing regimes and the FIPS 140-2 standard



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



Device Security Profiles

- A combination of the implementation of a chain of trust and the level of security robustness of the execution environment in the IPTV Device determines the specific ISS Security Profile associated with each model type of IPTV Device (ATIS-0800014.v002)
- The Device's Certificate (ISS/C) has extensions for specifying (and authenticating) device security profile
- A device security profile is given as the combination of its ISS Security profile and SEE sub-profile (e.g. ISS Profile 3-2). This example corresponds to a device in which:
 - ISS/A and ISS/E are indirectly verified (i.e. through software)
 - A Secure Execution Environment exists with high robustness (can only be defeated with great difficulty using professional tools) for:
 - the execution engine, storage, trusted paths, algorithms and secure time elements
 - Low robustness physical security exists (i.e. tamper detection only)



DRM APIs

- ISS has defined a rich set of DRM Server-side APIs
- These permit server-side middleware to interoperate with one or more DRM systems in the same network
- 52 Server-side APIs addressing:
 - IPTV Receiving Devices
 - Programs
 - COD Assets
 - Services
 - Service groups
 - Encryption/copy protection
 - Entitlements
- XML-based element definitions
- Work is underway on DRM Client-side APIs



IIF Device ID (work-in-progress)

- DeviceID = IPTVMfgID | MfgAssignedID
- IPTVMfgID: 6-byte Hex ASCII character field that uniquely identifies a manufacturer
- MfgAssignedID: Minimum of 6 and maximum of 58-byte characters taken from PrintableString set of RFC 5280 that uniquely identifies each device produced by a manufacturer



Work Currently Underway

- DRM Client-side APIs
- Managing the Trust Hierarchy (revocation and rules extension)
- Secure Time
- Device and Subscriber Identity and Authentication
- Security for COD Services
- Distribution of Content in the Subscriber's Authorized Service Domain
- VueKey Specification Review (APOD)



Putting It All Together – making CAS/DRM and devices interoperable in the Network

- CAS/DRM systems may interoperate in IPTV networks by:
 - Implementing the IDSA (ISS/S)
 - Using the DRM APIs
 - Implementing Simulcrypt interfaces
- Devices may interoperate in IPTV network security by:
 - Using the IIF DeviceID
 - Having certificates that are part of the IIF Trust Hierarchy (ISS/C, ISS/CA, ISS/R)
 - Implementing authentication and download/message encryption via ISS/A and ISS/E
 - Abiding by IIF Security Robustness Rules



An Open Framework

Ensuring IPTV's Interoperable Content Security

Speakers

Dan O'Callaghan



Vice Chair
ATIS IPTV Interoperability Forum
Member of the Technical Staff
Verizon Communications

Tony Wasilewski



Co-Chair
ATIS IPTV Security Solutions Committee
Distinguished Engineer
Service Provider Video Technology Group
Cisco Systems



Multi-Vendor Care Services

Reduced Complexity Ensures Optimal Efficiency

A Live ATIS Webinar - Thursday, July 15, 2010 | 11AM - 12PM ET

Register now at www.ATIS.org

Moderator



Lauren Layman
VP of Marketing & Public Relations

Speakers

Todd Wilson
Head of Care Services Delivery



Mike Mullineaux
Head of Services Marketing

Sponsored by

Nokia Siemens
Networks



For more information, please visit the ATIS Website at www.atis.org