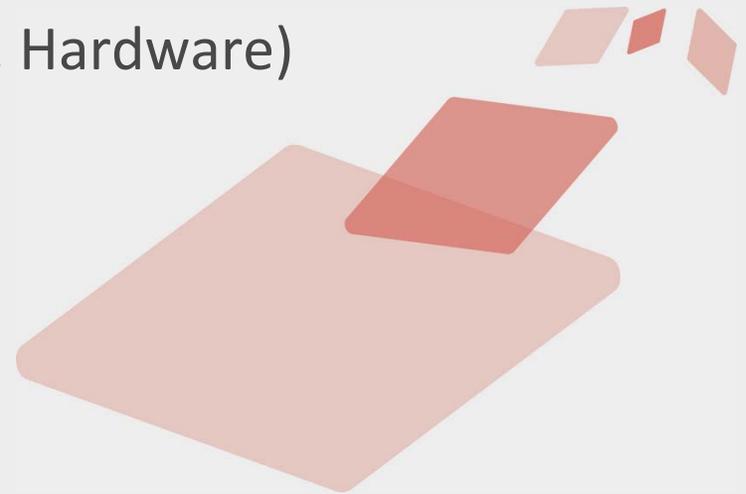


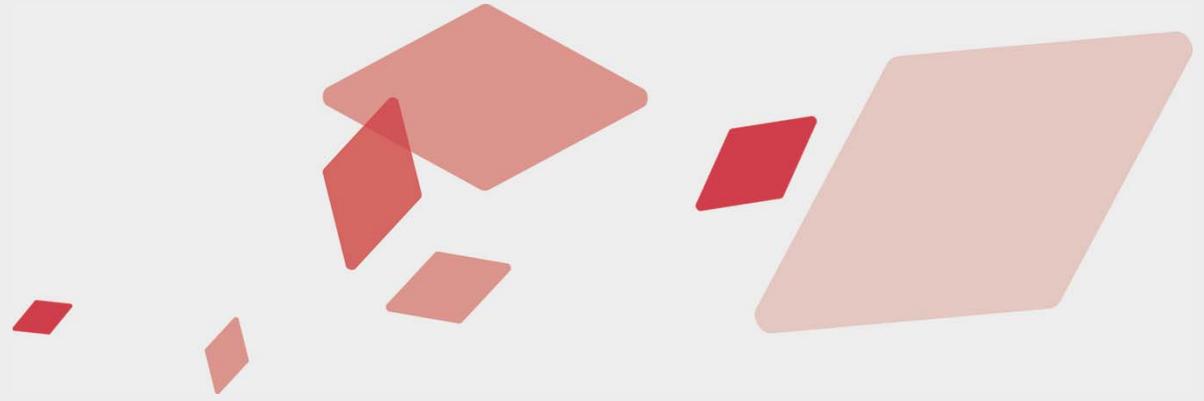
DSTAC Working Group Presentation

John B. Carlucci – President / CTO Alticast

Questionnaire Summary

1. Overview
2. Features & Functions
3. Components of Solution (Software, Hardware)
4. Technical Capabilities
5. Standards Used in the System
6. Deployment Model
7. Intellectual Property & Licensing
8. Porting Issues & Liability



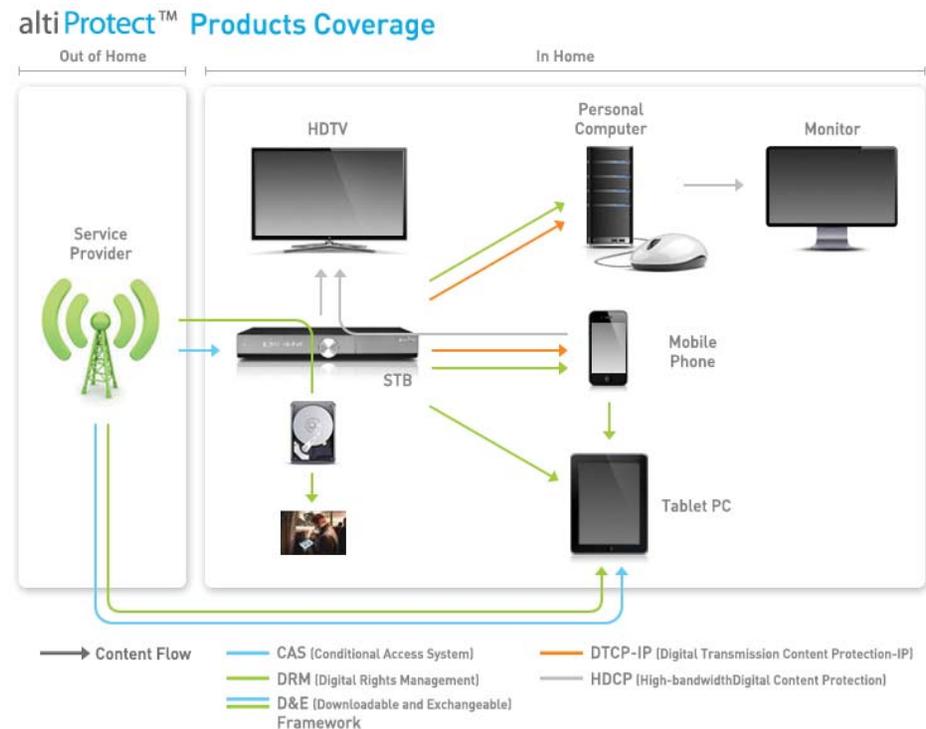


1. altiProtect Overview

altiProtect Overview

- altiProtect is a robust, scalable and cost-effective Security Solution delivering conditional access, digital rights management, and security distribution solutions that empower operators to secure premium content from piracy and unauthorized use

- Conditional Access, Digital Rights Management (DRM), Security Distribution and Digital Content/Copy Protection
- Service Protection – **altiProtect-CAS**
- Content/Copy Protection – **altiProtect-DRM**
- D&E Framework (Downloadable & Exchangeable) Framework – **altiProtect-D&E** Framework
- DCP (Digital Content Protection) – **altiProtect-DCP**



Value Proposition



- Proven Security
 - Telcordia Certified: 3rd party Security Assessment
 - Reinforce security based on powerful security module, altiTRS
 - Proven Track Record in the industry
- Compatibility & Flexibility
 - Cable, Satellite, and IPTV
 - SW only option with high portability to multi-device (phone, tablet) and multi-platform
 - Expandability of operator's business model based on downloadable solution
 - Successful Simulcrypt operation and replacement for legacy STBs
 - Applicable to legacy and next-gen environments, including emerging IP architectures
- Cost Effectiveness
 - Eliminating H/W dependencies including SmartCard and CableCard
 - » Offers decreased H/W and Maintenance costs for accelerated ROI
- Efficiency & Convenience
 - Improved operations efficiency through management consoles (Admin and Monitoring)
 - » Intuitive web based interfaces
- Continuous Support
 - Alticast is a business and technical partner for successful implementation of a provider's business goals

Security Flexibility – Ultra HD



- Stakeholders
 - Content Providers -> Requirements to Service Providers -> Supply Chain (Semiconductor, Hardware , Software , Security, Manufacturing, Operations)
 - Trust Authority / Industry Licensing Authority
 - » Contractual Agreements, Compliance, Robustness, Security Materials
 - » DCP, CA/DRM Provider ,OMS Licensing Authority
- MovieLabs' Ultra HD Requirements
 - AES-128 or Better
 - Decryption using individual device keys
 - Platform trust mechanism
 - HDCP 2.2 Link Protection
 - Hardware root of trust
 - Forensic Watermarking
- Example Requirement: HDCP 2.2 Link Protection
 - Digital Content Protection (DCP), LLC. , Licensing , Pricing, Security Material Distribution, Robustness Rules, Certification
 - Semiconductor Manufacturer, CPE Provider, Software Provider, Content Protection Provider

altiProtect-CAS Overview

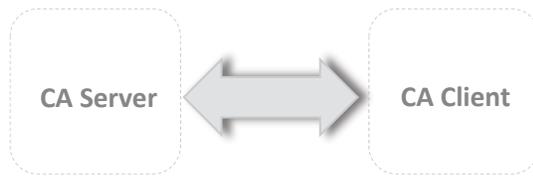


altiProtect-CAS is an optimized Conditional Access System for Pay-TV service

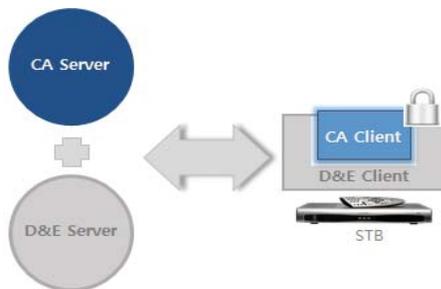
- altiProtect-CAS provides methodologies to protect content delivery to devices in the home via device verification and user authentication

Server based CA Solution – Two-Way Network

Apply on device with return path



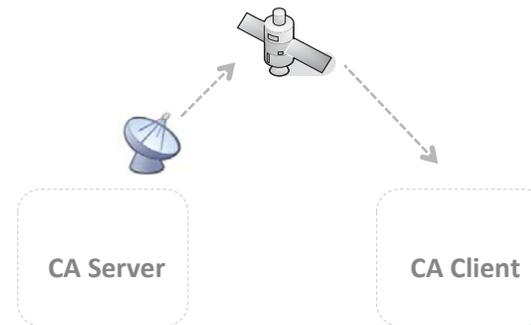
CA System + D&E Framework



S/W Framework for secure delivery and installation of CAS/DRM Modules

Secure-Micro based CA Solution – One-Way Network

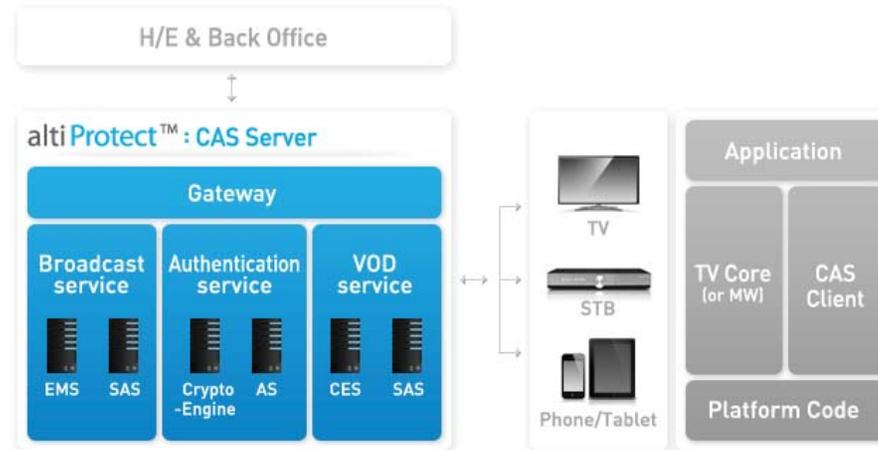
Apply on device without return path



altiProtect™ : CA Client



altiProtect-CAS Architecture



Server Group		Description
Broadcast Service	EMS (Entitlement Management System)	Channel Scrambling support : ECMG
	SAS (Subscriber Authorizing System)	Subscription Management : EMMG/EMMS
VOD Service	CES (Content Encryption System)	Session-based Encryption & Pre-Encryption support : SBV_ECMG
	CDS (Content Delivery System)	VoD Service support
Authentication System	AS (Authentication System)	Subscriber & Device Authentication
	Crypto Engine	Key & Private Information Management
Gateway		Interface with H/E : SMSGW, TCSGW, CMS

altiProtect-CAS Features



Main Features	Description
Entitlement Management	<ul style="list-style-type: none"> • Subscription Service <ul style="list-style-type: none"> – Multiple Subscription Service : Normal/Bonus Package, A La Carte, PPV • VoD Service <ul style="list-style-type: none"> – Real-time Scrambling (Session-based Encryption) for service protection – Pre-Encryption for contents protection • Package Purchase Service <ul style="list-style-type: none"> – ISU, OPPV/IPPV
Service Access Control	<ul style="list-style-type: none"> • Subscriber Group Control <ul style="list-style-type: none"> – Blackout/Spot control based on Region bit, Division bit, Zip code and Bouquet id • Parental Rating Control • Multi-Channel Control <ul style="list-style-type: none"> – Multi-Channel control for PVR, PIP, Multi-View service
Resource Management	<ul style="list-style-type: none"> • Package/Channel Management & Control <ul style="list-style-type: none"> – Package/Channel Management & Control Service through Interconnection with TCS & SMS • Subscription Management & Control <ul style="list-style-type: none"> – Subscription management & Control Service thru Interconnection with SMS
Copy Protection	<ul style="list-style-type: none"> • Copy Protection support <ul style="list-style-type: none"> – Macrovision/CGMS-A/HDCP control based on CCI
EMM Management & Monitoring	<ul style="list-style-type: none"> • EMM Management by Pre-defined Priority • EMM B/W Control & Monitoring • Auto Renewal support

altiProtect-CAS Features



Main Features	Description
Message Service	<ul style="list-style-type: none">Subscriber/Group/All-based OSD/B-Mail/Fingerprint Message Transmission Service
Reportback Service	<ul style="list-style-type: none">Reportback service<ul style="list-style-type: none">– On Demand/By Period/Event-based(i.e. PPV) Reportback
System Management & Monitoring	<ul style="list-style-type: none">System & Resource Status MonitoringLog Management & Monitoring
HE & Back-office Integration	<ul style="list-style-type: none">Multi-SMS supportSimulcrypt support
Others	<ul style="list-style-type: none">CAS Client Statuses Information Check service<ul style="list-style-type: none">– Hidden menu support for CAS Client status display

System Evolution via Simulcrypt



Simulcrypt Enabled Common Encryption & CP Migration

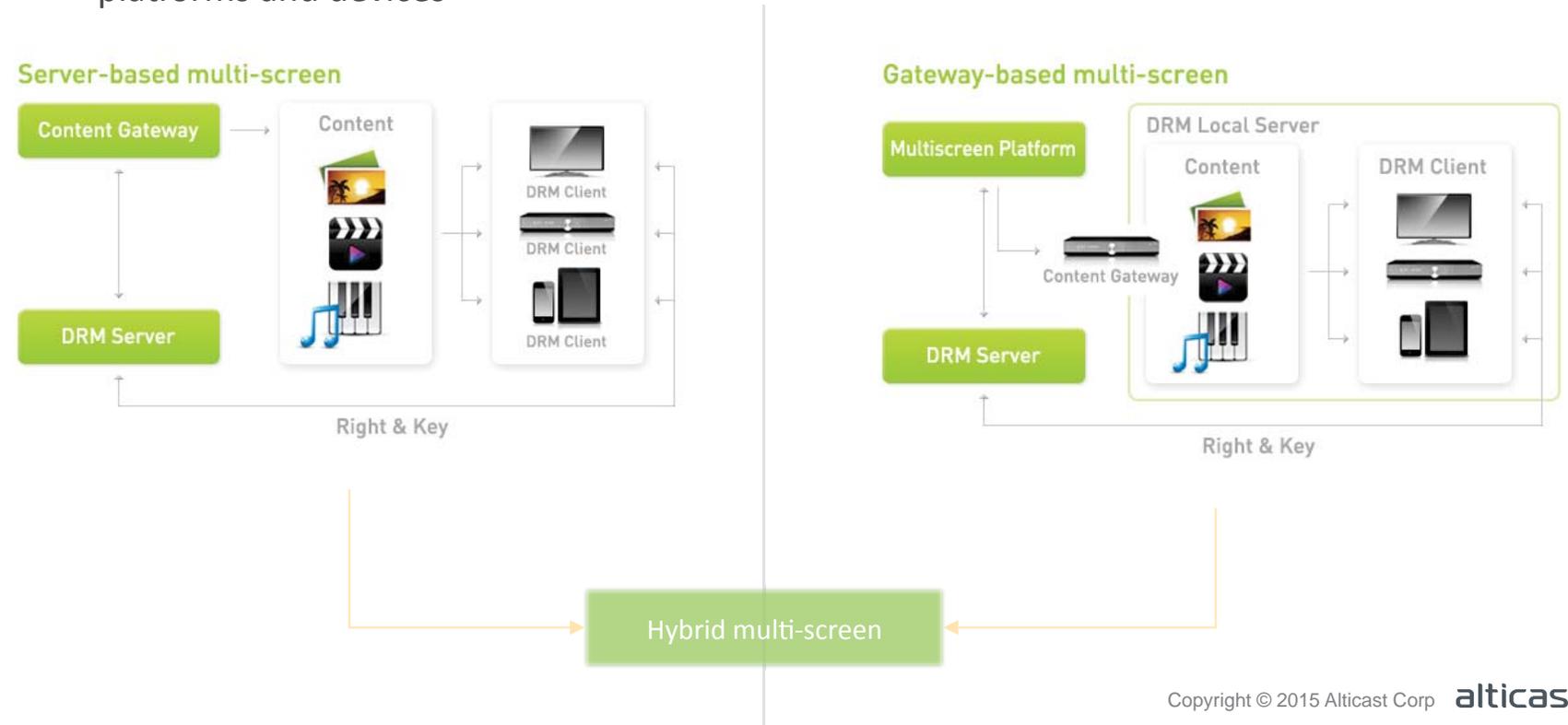
Deployed Service Providers	
Qrix <ul style="list-style-type: none">- altiProtect-CAS based on D&E Framework- System integration: simulcrypt- Service launched Nov 2009	Tbroad <ul style="list-style-type: none">- altiProetct-CAS based on D&E Framework- System integration: simulcrypt- - Service launched Jan 2010
KangNam Cable <ul style="list-style-type: none">- altiProetct-CAS based on D&E Framework- System integration: simulcrypt- Service launched Sept 2010	Jeju Cable <ul style="list-style-type: none">- altiProetct-CAS based on D&E Framework- System integration: simulcrypt- - Service launched Nov 2010
ChungBook Cable <ul style="list-style-type: none">- altiProetct-CAS based on D&E Framework- System integration: simulcrypt- Service launched March 2011	CJHV <ul style="list-style-type: none">- altiCAS+altiXCAS- System integration: simulcrypt- - Service launched Oct 2014

altiProtect-DRM Overview

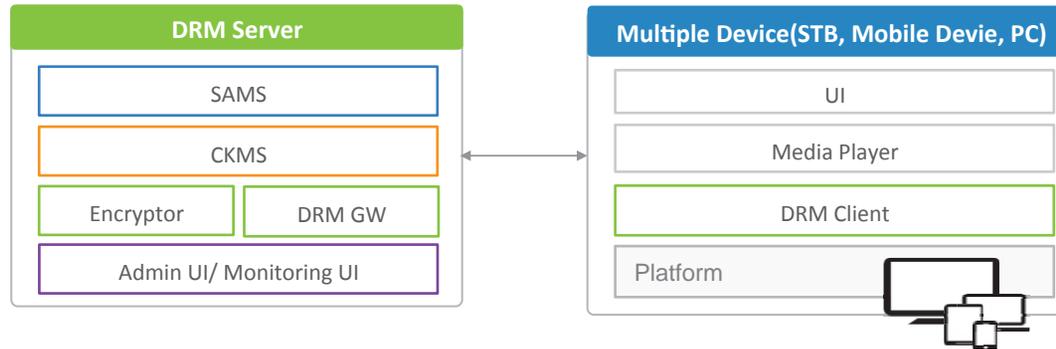


altiProtect-DRM is a proven Digital Rights Management and Protection solution for paid content on bi-directional IP and Cable networks

- altiProtect-DRM blocks the illegal copy and distribution of content serviced on multiple platforms and devices



altiProtect-DRM Architecture



DRM System	Modules	Description
SAMS (Subscriber Authentication and Management System)	• AS (Authentication Server)	• Authentication & Certification Download Server
	• LS (License Server)	• License(Including Authorization) Issue Server
	• DIS (DRM Interface Server)	• Proxy Interface Server between DRM Server and DRM Client
CKMS (Certification & Key Management System)	• CIA (Cert Install Agent)	• Certificates Generation and Management
	• LSM (License Server Manager)	• System License Management
Encryptor	• aEL (altiProtect-DRM HLS Encryption Library)	• Content Encryption Support
DRM G/W	• DRM G/W(DRM Gateway)	• Interface Server between 3rd party System and DRM System
AUI/ MUI	• Admin UI	• Admin Console for Operators
	• Monitoring UI	• Monitoring Console for Operators

altiProtect-DRM Features



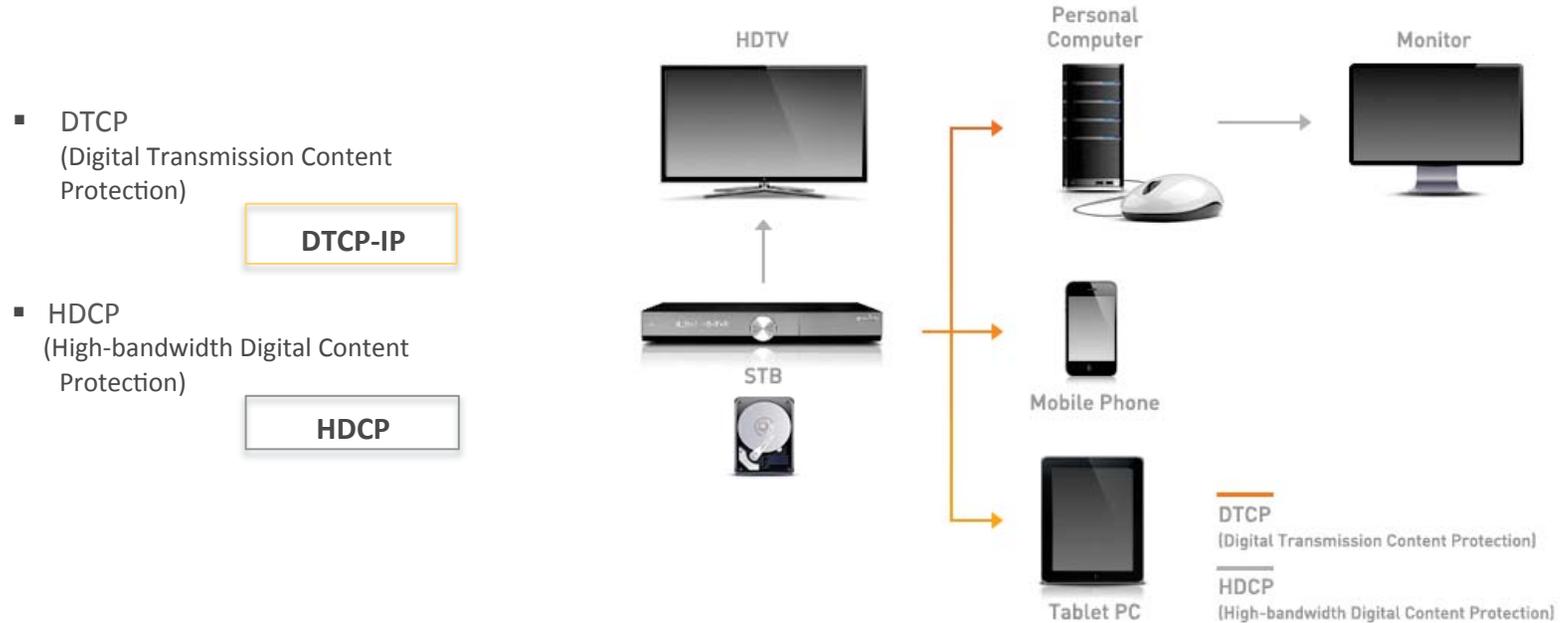
Main Features	Description
Content Protection	<ul style="list-style-type: none"> • Anywhere, anytime, any device <ul style="list-style-type: none"> – Confidentiality of contents – Integrity of data
Contents Sharing	<ul style="list-style-type: none"> • Contents sharing with family and friends <ul style="list-style-type: none"> – On-line sharing – Off-line sharing
Contents Access Control	<ul style="list-style-type: none"> • Based on Rights and License <ul style="list-style-type: none"> – Playback/Record – Count, Date-time, Interval, Accumulated • Parental Rating Control • PIN control and management
Subscriber and Device Authentication	<ul style="list-style-type: none"> • Subscriber and Profile Log in/out management • Device authentication based on X.509 certificate • Mutual Authentication between DRM Server and Client
Contents Encryption	<ul style="list-style-type: none"> • Real-time encryption support • Pre-encryption support
Subscription Management (Domain Management)	<ul style="list-style-type: none"> • Rights and Domain based on; <ul style="list-style-type: none"> – Subscriber (Family Domain) – Profile (Personal Domain) – Device
Contents Management	<ul style="list-style-type: none"> • Content and License Mapping
License Management	<ul style="list-style-type: none"> • Various License Management
Certification and Key Management	<ul style="list-style-type: none"> • Certification generation & management • Contents Encryption Key management • Subscriber based Key Info management

altiProtect-DCP Overview



altiProtect-DCP(Digital Content Protection) is a Link Protection solution for copy protection within a user's home network

- Enabling Link Protection between standard compliant devices



altiProtect-DCP Applications



DLNA with DTCP-IP



Wi-Fi Certified Miracast™ with HDCP



altiProtect-DCP Features



Type	Main Features	Description
DTCP	Link Protection	DTCP-IP : Mapping DTCP to IP
		Device Authentication and Key Exchange(AKE)
		Content Protection
		Content Copy Control based on CCI(Copy Control Information)
		System Renewability
HDCP	Digital Copy Protection	Authentication and Key Exchange (AKE)
		Locality Check
		Session Key Exchange (SKE)
		HDCP Encryption

Downloadable Experience - XCAS/NCAS



- Why Downloadable?
 - Reduced Power Consumption
 - Compact Form Factor
 - Field Upgradable

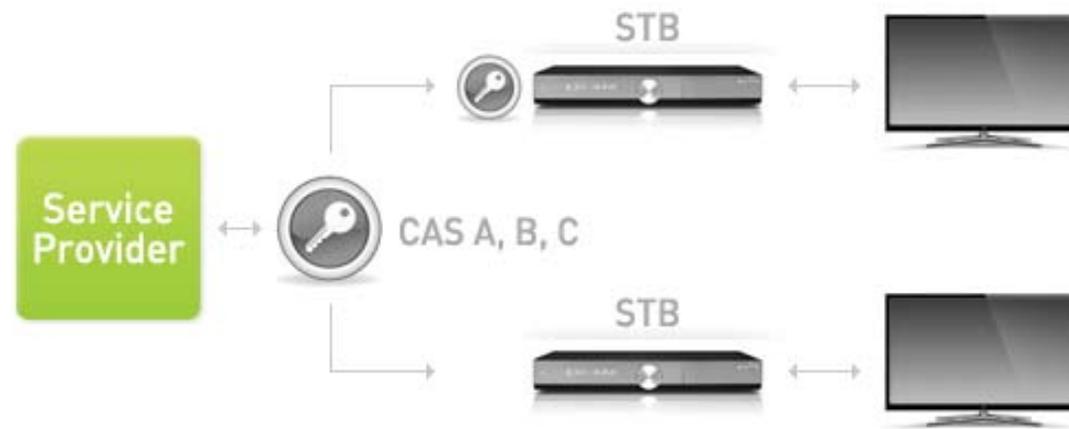
Solution (Location)	Cablevision JCAS (USA)	CableCard Replacement (Korea)	CableCard Replacement (USA)
Device SW	OCAP Software	OCAP Software	Native Stack via DLL
Security Client	Java API	KLAB Java API	NCAS API
Download Mechanism	OCAP Carousel	XCAS	Flexible

altiProtect-D&E Framework Overview



altiProtect-D&E (Downloadable and Exchangeable) Framework is an optimized security framework for downloading and exchanging CAS/DRM client modules based on a bi-directional network

- Multi-CAS/DRM Support
- Korea National Standard compliant



altiProtect-D&E Framework Architecture



Component		Description
XCAS Server	AP (Authentication Proxy)	• Interface between D&E Framework Servers and Client in Host
	LKS (Local Key Server)	• Certificates and Key Management
	PS (Personalization Server/Provisioning Server)	• CAS/DRM Client Image and Personalized Information Management
	DMS (D&E Multicast Server)	• Transmission of triggering messages for authorization and downloading CAS/DRM Client
	Gateway	• Interface between D&E Framework Servers and SMS
XCAS Client	D&E Manager	• Message mediator in XCAS STB
	D&E SM (Secure Module)	• Core module of D&E Framework clients • Mutual Authentication between AP ↔ SM and SM ↔ TP
	TP (Transport Processor)	• Descramblers

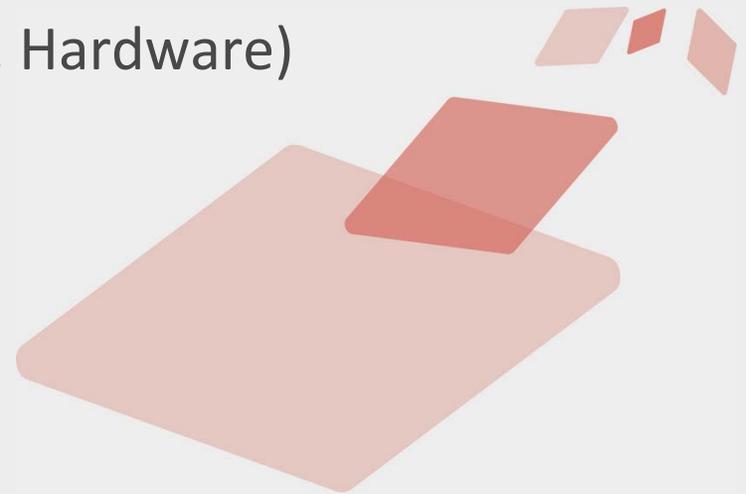
altiProtect-D&E Framework Features



Features	Description
Mutual Authentication	<ul style="list-style-type: none">• Mutual authentication between AP and SM for Device authentication<ul style="list-style-type: none">– Initial Authentication for Initial device authentication– Typical Authentication• Mutual authentication between SM and TP in Device
Secure CAS Client Download	<ul style="list-style-type: none">• Secure CAS/DRM client download onto the authenticated device.<ul style="list-style-type: none">– 1 step : Typical Authentication between AP and SM based on Certificates– 2 step : the encrypted CAS/DRM client download through the secure channel
Image Management	<ul style="list-style-type: none">• Personal / Group / All based Image download and Management according to Service Operator's security policy
Reportback	<ul style="list-style-type: none">• On-demand reportback service<ul style="list-style-type: none">– Device status– Encrypted log for detection of critical errors
Various Client Type support	<ul style="list-style-type: none">• CAS/DRM/ASD support

Questionnaire Summary

1. Overview
2. Features & Functions
3. Components of Solution (Software, Hardware)
4. Technical Capabilities
5. Standards Used in the System
6. Deployment Model
7. Intellectual Property & Licensing
8. Porting Issues & Liability



2. Features & Functionality



- Security Functions: CA, DRM, Link Protection, Water Marking, Device & User Authentication & System Renewal
- Networks Supported: All two-way Networks
- Service & Device Functions: Live, File & Progressive VOD, PPV, Download Rental, Local Recording, Output Control, Whole Home Streaming
- Device Support: Special Purpose & Generic Consumer
- Application Support: CA APIs for Purchases & Other Operations, Billing Gateway

3. Components of Solution



- Software:
 - Downloadable: CAS Client
 - Trusted Execution Environments (TEE): TrustZone, SAGE, & Protected Media Path (PMP)
 - Download Code Verification, Update, Signing: Signed with TA/ ILA provided Certificates,
 - Software Rollback Support: Yes
 - Application Interfaces: Java, Native, JavaScript

3. Components of Solution



- Hardware:
 - Physical Platform: Secure Key, OTP, Crypto Functions, or OMS KLAD
 - Secure Element Access: CA APIs
 - CPU or CPU Architecture: No specific Requirements
 - Physical Element Absent: Subset of functions provided
 - Robustness & Compliance Rules: Trust Authority
 - 3rd Party App Supported Independent of CA: Yes
 - 3rd Party App Independent Lab: No
- Device ID & Keying
 - Secure Mechanism for ID: Yes
 - Serial Number Unique ID Requirement: Yes
 - Key Storage Capability: Yes
 - Standardized Communication w/ SOC: Yes
- Key Server/Client Communication
 - Two-way: Yes. Full Time: No
 - Secure Channel: Yes. IP Not Required.

4. Technical Capabilities



- Transport Formats: All
- Content Delivery: All including HFC QAM, IP Unicast, IP Multicast
- Network Information (Service Information): Required for tuning live channels
- Ciphers Supported: Independent of Cipher (e.g. DVB_CSA, AES, DES, SCTE-55)
- App APIs: Decryption Request & Entitlement Query

5. Standards



- Standard Ciphers, Transport & Networking
- ETSI TS 103 162/SCTE 201 2013
- Korea Digital CableLabs XCAS/ICAS
- W3C EME /SME
 - Webkit Open source Derived Browser
 - Stabilize (March 31 2015) to consider timing on how to incorporate into solutions.

6. Deployment Model



- Transmission Network: Existing & Transmission Independent
- Large Cost Elements: Variable
- Co-Existence w/ Legacy: Simulcast or Simulcrypt

7/8 Intellectual Property & Porting



- 7. Licensing
 - Trust Authority / ILA Specifics Licensing Terms
 - Alticast Solution Components are Licensed
- 8. Porting
 - Content Protection Provider Performs port of Client. Software Provider performs port of Device Software.
 - Validation based on TA/ ILA Robustness Rules and Licensing
 - Indemnification based on Licensing and Commercial Terms

Thank You!