REDEFINING CONTENT SECURITY WHITEPAPER SERIES

TRANSFORMING PAY-TV WITH HYBRID IPTV/OTT SECURITY SOLUTIONS

conax.com

CONTENTS

INTRODUCTION

The pay-TV market is currently torn between meeting the consumer demand for new and innovative services while at the same time cutting subscription fees due to increased competition. Next-generation pay-TV customers, especially Millennials, expect more flexibility in their pay-TV services and are increasingly cutting the cord to save money.[1]

To be successful in today's market, operators must offer a rich user experience with a variety of ways to consume television content with time-shift TV, VOD, search and recommendations, third-party streaming services and PVR delivered to a multitude of devices. Many of these customer requirements emerge faster than traditional pay-TV operators are able to react, enabling streaming companies such as Netflix, Hulu, and Amazon to directly compete with their offerings. Adapting quickly to market changes and launching new services ahead of the competition while keeping costs under control is increasingly important.

Network-wise, there's a monumental transition underway in the pay-TV industry. Satellite and terrestrial service providers are adding OTT to their existing platforms. Cable operators are migrating to all-IP with DOCSIS3.x and Fiber to the Home (FTTH), and telcos are integrating multicast IPTV and on-demand OTT content on a single, multi-device service delivery platform.

As cable operators are seeking to capitalize on the revenue opportunities presented by IPTV, one of the challenges they face is content protection.[2] *Content security is still hugely important when acquiring the most attractive content, protecting the service from ransom attacks and ensuring the quality of service. This whitepaper identifies the key capabilities that IPTV service providers should look for in a content security solution to ensure secure distribution of broadcast television content to managed connected devices.*

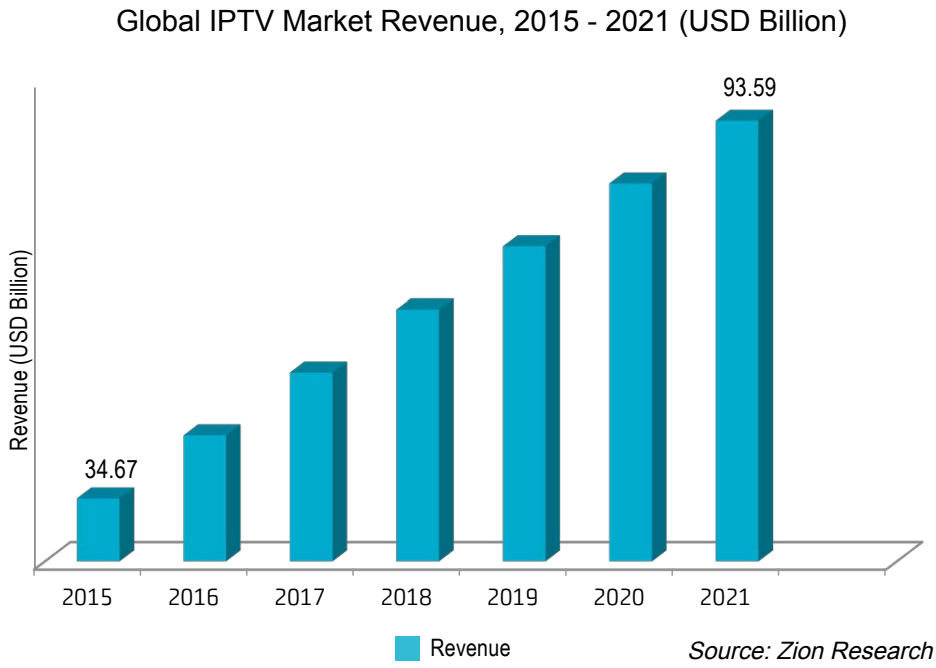
---

[1] *http://www.ooyala.com/users/videomind/blog/41-customers-surveyed-said-they-ll-cut-cancel-pay-tv*

[2] *https://www.abiresearch.com/market-research/product/1022742-pay-tv-and-ott-piracy-prevention-services/*

THE HISTORY OF IPTV

The IPTV market is poised for significant growth. According to a recent report from Zion Research, the global IPTV market will grow in value from $34.67 billion in 2015 to $93.59 billion in 2021, a CAGR of around 18.01 percent between 2016 and 2021.[3] To understand why researchers are predicting a boom in IPTV subscriptions, a brief history of the underlying technology is important.



Source: Zion Research Analysis 2016

Introduced in the mid-1990s, IPTV (Internet Protocol Television) is television content that is delivered to homes via an IP network as opposed to satellite, cable or terrestrial networks. The biggest difference between IPTV and traditional delivery methods is that the latter were designed as a one-way broadcast system, whereas IPTV enables two-way services. With IPTV, service providers can integrate television with other IP-based services, like high-speed internet, VoIP, and interactive TV offerings.

Currently, broadband deployments are increasing globally. As service providers look to deliver more interactive services, such as VOD, time-shift TV, and pay-per-view, IPTV has become a cost-effective and dependable solution for delivering a next-generation television experience.

Unlike streaming video over the open internet, IPTV is typically powered by operator managed high-performance, secure networks, thereby ensuring a reliable end-user experience. From a bandwidth perspective, multicast IPTV offers an advantage over traditional delivery approaches. Content remains within the operator managed network, and only the content the customer selects is sent to the home, freeing up bandwidth.[4]

Given its benefits and the recent changes in television consumption, IPTV is penetrating every region around the world, albeit some more rapidly than others. Transparency Market Research reports that falling IPTV subscription prices and expanding broadband penetration have made Western Europe the strongest

[3] *http:// www.marketresearchstore.com/news/global-iptv-market-245*
[4] *http:// en.wikipedia.org/wiki/IPTV*

overall market for IPTV in terms of revenue generation[5]. Asia Pacific is estimated to be the fastest growing regional segment of the global IPTV market in the coming years, with South Korea, India, Indonesia and China being the largest contributors. In fact, the region of Asia Pacific excluding Japan is projected to register a CAGR of 21.1 percent during the forecast period of 2014 to 2020. Latin America, the Middle East and Africa are also expected to exhibit significant growth over this period. Digital TV Research estimates that IPTV subscriptions are growing faster than any other pay-TV form in the MENA region, and that IPTV revenues there could grow 10 times by 2020.[6]

Why the dramatic increase in IPTV subscriptions? Transparency Market Research noted that the growth of the IPTV market can be attributed to surging demand for HD channels and video on demand, combining interactive services with IPTV services, and government initiatives across the globe.[7]

Given the abundant growth and changes underway in the IPTV market, what types of security solutions should service providers seek out? The next sections will explore this issue.

FLEXIBILITY IS KEY IN BEING FUTURE PROOF

To handle the ever-evolving nature of the pay-TV world, operators need a security solution that first and foremost is flexible, both from an integration and deployment perspective. In-the-field retrofitting and pre-integration into the STB are also must-have capabilities. Let's take a closer look at the features that are absolutely critical in a modern security solution.

SPEED UP CONTENT SECURITY INTEGRATION

Time-to-market is everything in the pay-TV world. If it takes an operator months or years to introduce a new TV platform or device, it's likely that they're behind the competition. From a content security viewpoint, how can operators speed up the STB integration process?

To enable shorter time-to-market and facilitate the integration of the security client in a STB for premium services, like Ultra HD (UHD), pre-integration of hardware separated software components is vital. Security vendors working closely with system on a chip (SoC) vendors are able to provide this type of separation and, in turn, enable STB manufacturers and operators to quickly deploy secure STBs with the ability to offer high-value content.

Pre-integrating the security client onto the trusted part of STB chipsets enables a shorter time to market for pay-TV services.

INTEGRATION FLEXIBILITY

Complexity can also be reduced by using a security client that can be integrated in the STB and chipset to perfectly suit the hardware and software resources. Based on security requirements, operators can utilize different hardware and software technologies, such as Rich Execution Environment (REE), Trusted Execution Environment (TEE), and additional security on separate and proprietary areas of the STB chipset.

[5] *http://www.businesswire.com/news/home/20150406005280/en/IPTV-Market-Stimulated-Increased-Broadband-Penetration-Transparency*
[6] *http:// www.ooyala.com/videomind/blog/4x-growth-cloud-tv-revenues-2019-iptv-revenues-more*
[7] *http:// www.businesswire.com/news/home/20160303005024/en/Growth-Interactive-Services-Expected-Boost-IPTV-Market*

Rich Execution Environment (REE)

The REE is the general area of the chipset where most processes are managed. This is the area of the STB where the middleware, third-party apps, operator apps and most other general software, are executed. The security operations can be implemented and executed in REE.

Trusted Execution Environment (TEE)

The TEE is a secure, integrity-protected processing environment inside the main processor (SoC), where both security sensitive operations are run, and sensitive data is kept separate from the REE.

FLEXIBILITY TO IMPLEMENT DIFFERENT SECURITY LEVELS

Ultimately, operators need a security solution that can be adjusted to fit all of the different security levels and requirements from content owners. Operators can tailor the security client and STB resources to fit each security level. For example, operators can decrease the resources used in a STB for deployments without high-end security demands to reduce their expenses. When it comes to STBs deployments with higher requirements, the security level can be strengthened, as needed by utilizing more security hardware resources. For instance, when an STB is used for SD content, additional hardware resources would typically not be required and the conditional access (CA) client can be implemented with less costly chipsets. To deliver high-end content, such as UHD and early release (i.e., Hollywood movies that are distributed digitally, ahead of DVD and Blu-ray), the inclusion of very strong security with physical separation of CA operations from middleware in the STB is a necessity. (See our white paper on 4K for more information http://www.conax.com/white-paper-on-4k-security/.) In this case the security solution needs to be implemented with more resources in the chipset and software in the STB.

To quickly adapt to new technologies and launch new service offerings with speed, operators need a security solution that is flexible, not a one-size-fits-all solution. The security client should be adaptable on multiple levels and offer different degrees of security. Using a security client that has an adaptable approach to integration allows operators to optimize the STB integration through use of standardized APIs. If the client can reuse the API integration done with the middleware in the REE, integration efforts are greatly reduced when adding new STBs with other hardware in the same operation. This way, the same middleware integration is reused on STBs from different manufactures and on those devices with different security levels.

DEPLOYMENT FLEXIBILITY

The most common way to integrate a new security client in a STB is in the factory during production. Doing this the operator is able to utilize the hardware capabilities in the STB and increase the security level. Having an increased security level is a prerequisite for most of the premium content. But sometimes it is highly beneficial to reuse the existing deployed STB population when introducing content security in an unsecure operation or replacing the existing content security solution.

To reduce time to market and lower CAPEX when adding or replacing security solutions in existing pay-TV operations, operators should choose a security solution that can be reused on already deployed STBs.

IN-THE-FIELD RETROFITTING

Choosing a software solution that can be deployed remotely on STBs gives operators the ability to retrofit existing devices, meaning they can update or change their security solution in the field. Operators can easily replace existing security solutions without making a large investment in new STB hardware.

Let's say an operator has 2 million customer households with an IPTV STB, and the security solution needs to be replaced. With a software-based client, security updates can be sent over the air to the STB. There's no need to purchase 2 million new STBs or bring the devices into a warehouse for retrofitting.

BENEFITS OF A HYBRID SECURITY CLIENT

Nowadays, many operators are complementing their existing platforms with OTT-delivered offerings to remain competitive and add value to their service. Often, this has resulted in multiple service delivery and content protection systems being used. To securely distribute linear and nonlinear content across a variety of networks (e.g., IPTV, DVB and OTT) to the STB, operators require both CA and Digital Rights Management (DRM) technology. Using two or more separate CA and DRM systems requires multiple integration efforts, multiple sets of security requirements and certifications, and multiple headend servers. Aside from being complex, it can be an expensive undertaking.

Selecting a security solution that can handle a range of distribution technologies, from IPTV to connected DVB and adaptive bitrate (ABR) streaming is both cost-effective and operationally effective. One solution serves a dual purpose, providing operators with a traditional CA system for delivery of linear TV channels and VOD, and simultaneously a DRM client that enables ABR streaming in various formats like MPEG-DASH and HLS to the same STB.

Increasingly, operators are moving toward using ABR as the delivery mechanism for on-demand content because they want to provide the same content on STBs and secondary screens like tablets and smartphones without duplicating their content workflow, processing and storage. Not only do storage costs decrease when operators use one security solution for IPTV/DVB/ABR delivery, but the entire content workflow is simplified from ingestion to metadata handling and more. Let's say an operator has a standard IPTV security solution and they want to begin offering OTT content on the same STB. Typically, they would need to employ a DRM solution alongside the CA system. While there are some security clients on the market that offer a single solution for CA and DRM, the majority require separate, higher integration costs. Operators would benefit from and be prepared for the future with a solution that can implement both security technologies through a single integration process.

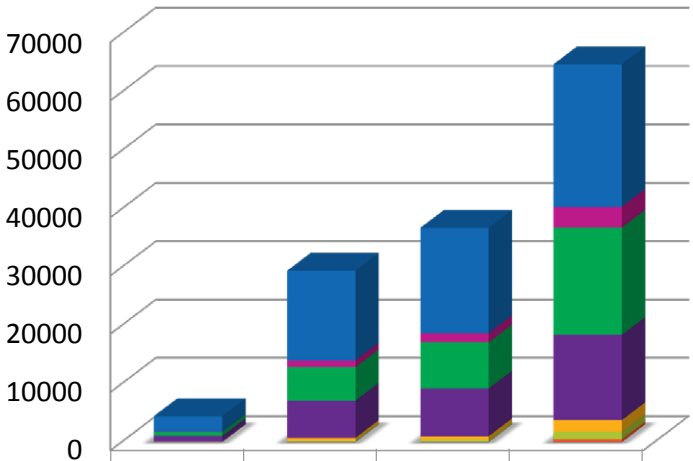
HANDLING IPTV AND OTT DISTRIBUTION TECHNOLOGIES

As the video distribution trend moves toward using OTT streaming technologies, such as MPEG-DASH and HLS, it is important for pay-TV operators to ensure they can deliver content in a manner that optimizes their reach and supports the business models that the customers want. Moving some pay-TV services to OTT streaming technologies allows operators to utilize the same content across platforms.

Operators must choose a security solution capable of securing OTT content on STBs if they want to distribute content via MPEG-DASH and HLS protocols to customers on managed and unmanaged devices. This approach is beneficial for operators that want to offer services like on demand, time-shift TV, and linear content to more devices without duplicating content assets, while still maintaining the control of the end-user offering and keeping the focus on customer satisfaction and loyalty. To ensure a seamless transition from pure IPTV services to hybrid offerings of IPTV and OTT, the security client for STBs should be able to handle both sets of technologies, and thus eliminate the need for additional integration and complexity. With the ability to secure OTT content on STBs, operators can capitalize on global OTT TV and video revenues, which are expected to grow up to $64.8 billion by 2021, according to Digital TV Research.[8]

[8] *http://www.streamingmediaglobal.com/Articles/News/Featured-News/OTT-Video-Revenue-to-Swell-to-$65-Billion-Worldwide-by-2021-112394.aspx*

Global OTT TV & Video revenue forecasts by region (USD million)



	2010	2015	2016	2021
North America	2674	15389	18078	24387
Latin America	32	1152	1596	3586
Asia Pacific	707	5741	7894	18396
Europe West	1014	6396	8199	14642
Europe East	26	454	633	1976
MENA	13	255	339	1328
Sub-Sahara Africa	0	22	37	467

Source: Digital TV Research

UNIFIED SECURITY BACK-END

As a multi-network service provider, offering a unified protection environment across all devices, networks and use cases is no small task. The best way that operators can minimize CAPEX and OPEX, as well as streamline the transition to IP, is to use a single back-end for all their security needs, whether they are delivering content over DVB, IPTV, or OTT networks.

We recommend utilizing a security solution with a back-end that can handle all types of pay-TV distribution. The back-end should support any and all combinations of one-way broadcast, two-way broadcast, IP-based distribution and ABR streaming on STBs. In addition, the back-end needs to offer ABR streaming on open devices like tablets, smartphones and browsers through native DRM (multi-DRM) functionality.

CONCLUSION

As the IPTV market grows and operators contemplate introducing additional offerings, like OTT, multiscreen, and time-shift TV, having a flexible, cost-efficient, and scalable content security approach becomes ever more critical. Given the variety of distribution networks, device types, and content security requirements that are involved with delivering a premium television experience, operators need a solution that will speed up time to market, not slow it down. Conax offers a winning solution.

OUR UNIQUE APPROACH: UNITING THE CONTENT SECURITY CLIENT AND BACK-END

For over 25 years, Conax has provided the pay-TV market with reliable, affordable, and flexible content security solutions. In 1990, we designed one of the first pay-TV smart cards, and the rest is history. Since then, we've kept our fingertips on the pulse of the industry, responding to operators' needs for flexible solutions that ensure content protection for any device, anywhere, any time.

CONAX OFFERS A LEVEL OF FLEXIBILITY THAT CAN'T BE MATCHED.

Conax Connected Access is a multi-purpose premium security client tailored to eliminate the complexity of securing a modern pay-TV service, allowing operators to support both CA and the DRM protection for content delivered on hybrid STBs. Regardless of the security requirements, operators can strengthen content protection and easily adapt to changes via Connected Access, supporting SD to HD and up to 4K scenarios. Using Connected Access with Conax Contego, our unified security back-end, operators can dramatically speed up the time to market for new IPTV features and services, including live TV, on-demand, PVR, and catch-up TV.

Conax Connected Access is ideal for new operators entering the IPTV market, as well as existing broadcast operators going IP through technologies like DOCSIS 3.x, xPON, FTTx, 3G/4G or LTE/5G. When combined with Contego, Connected Access makes operators exceptionally well-equipped to protect content across all devices, distribution networks and use cases. Security levels can be adapted to address available device capabilities.

Through its flexible architecture, simple integration process, and ability to retrofit on deployed STBs, Connected Access reduces CAPEX and OPEX, guaranteeing the protection of content delivered over connected DVB, IPTV, or OTT networks utilizing available security mechanisms like hardware-root-of-trust with chipset pre-integrations. Uniting IPTV and OTT in one single STB client, Connected Access gives IPTV operators a competitive edge in today's connected television world.

For more information, visit:
http://www.conax.com/products-solutions/conax-secure-clients/conax-connected-access/ and *http://www.conax.com/products-solutions/conax-security-platform/contego/*.

Interested in becoming a Conax partner? Contact: partner@conax.com

Request a demo or visit from us? Contact: info@conax.com

Need more information on Conax solutions ?

www.conax.com | info@conax.com | T: +47 22405200

About Conax

A part of the Kudelski Group, Conax is a leading global specialist in total service protection for digital TV and entertainment services via broadcast, broadband and connected devices. The Conax Contego unified security hub provides telcos, cable, satellite, IP, mobile, terrestrial and broadband operations with an innovative portfolio of flexible and cost-efficient solutions to deliver premium content securely. Conax' future-ready technology offers modular, fast-time-to-market solutions that enable easy entry into a world of secure multiscreen, multi-DRM content delivery and secures rights for premium content delivery to a range of devices over new hybrid network combinations. Conax spotlight technology includes award-winning Conax GO Live and benchmark Conax multi DRM security, and includes Conax Connected Access connected IPTV security client managing both Conditional Access and DRM security in one single client for reduced operational complexity and cost. Headquartered in Oslo, Norway, ISO 9001 & 27001 certified Conax technology enables secure content revenues for 425 operators in 85 countries globally. For more information, please visit www.conax.com and follow us on Twitter, LinkedIn and Facebook to join in the conversation.