technicolor

FEEL THE WONDER

ホワイト・ペーパー

ビデオ・コンテンツ保護とAndroid TV

統合を軽視しないでください！

内容

© Copyright 2018 Technicolor.2018年11月22日

前書き

30年以上にわたって使用されている有料テレビ放送とビデオ配信サービスを可能にしたのは、プレミアム・コンテンツへの消費者アクセスを制御し、収益化を実現するための必須機能であるアクセス制御技術でした。初期にビデオ配信ネットワークでは片方向のブロードキャスト通信だけが可能でしたため、限定受信方式（*CAS*）とも呼ばれるこのアクセス制御技術は、すべてのデジタル・テレビ放送規格で使用されているMPEG-2トランスポート・ストリーム層の上層に使用されるように設計されました。しかし、IPネットワーク上での線形およびオンデマンド型のビデオ配信の普及により、デジタル著作権管理（*DRM*）と呼ばれる代替アクセス制御技術が市場に登場し、その重要性が高まりました。また、適応ビットレート（*ABR*）ストリーミング技術とIPネットワークの双方向通信が利用れました。

GoogleがAndroid TVプラットフォームを発売した2014年には、新たに定義されたカテゴリのAndroidデバイス（つまりテレビ・デバイス）の基盤となるオペレーティング・システムとしてAndroidが利用されました。他の多くのIPビデオ・プラットフォームと同様に、初期にAndroid TVは、IPネットワークを介して配信されるオンデマンド型のオーバーザトップ（*OTT*）ビデオ・ストリーミング・サービスに注目しました。また、TV入力フレームワーク（*TIF*）のおかげで、フックを使用して無料の線形テレビ放送チャンネルをサポートすることができました。しかし、過去2年間で、オンデマンド・ビデオに加えて有料の線形テレビ放送をサポートするハイブリッドAndroid TVテレビ・デバイスに対する需要と重要性が劇的に高まったため、Android TVにCASソリューションを統合する必要性も高まっています。

偶然にも、Android TVの発売と同時に、超高解像度（*UHD*、*4K*とも*呼ばれる*）が登場したし、米国の大手映画会社のほとんどが運営する映画製作所であるMovieLabsは、拡張コンテンツ保護（ECP）に対する独自の仕様を発表しました。もうお分かりのとおり、コンテンツの著作権所有者は現在、プレミアム・ビデオ・コンテンツのアグリゲーターおよび配信業者が著作権のある作品の違法な複製および再配布を防止するための可能な全ての処置を取ることを要求しており、消費者のデバイスにECP仕様に記述されている技術を統合して消費者のデバイスがユーザーに対して透過的であるようにすることを勧めています。これらの要件は、最新世代のCASおよびDRMソリューションの実装方法に非常に大きな影響を与えます。

このような市場動向と技術発展のために、すべての事業者およびコンテンツ・プロバイダーは現在、消費者のビデオ・デバイスで最新のアクセス制御技術を素晴らしい方式で実装することを要求しています。このような期待を満たすには、少数の企業だけが持っている経験とスキルが必要です。以下ではその理由と最新のアクセス制御技術の実装方法を説明しています。

© Copyright 2018 Technicolor 2018年11月22日

CASおよびDRMソリューションの概要

限定受信方式

ペイTVで初期に展開されたすべての限定受信方式の主要特性と動作原理は同じです。限定受信方式の主要特性と動作原理は次のように要約できます：

- 限定受信方式は、放送ネットワークを介して配信される貴重な線形オーディオ/ビデオ・コンテンツを保護するために設計されたエンドツーエンドのソリューションです。コンテンツ保護は、線形TVチャンネルを伝送する前にリアルタイム・モードで線形TVチャンネルにスクランブルをかけることによって実現されます。
- ブロードキャスト配信ネットワーク上で安全なコンテナ（通常ECM、資格制御メッセージとも呼ばれる）を介してすべての受信デバイスに渡されるスクランブリング・キー（頻繁に更新される）に依存する対称スクランブリング・プロセスが使用されます。受信側の消費者デバイスはコンテンツのスクランブルを解読することができます。
- すべての受信デバイスにデータを送信する配信ネットワークではユーザーの受信デバイスのIDと認証情報を遠隔で確認することができないため、デバイスに固有識別子を組み入れ、他のセキュリティ機能を統合することで、ローカルで、受信デバイスを安全に識別し、ユーザーにコンテンツへのアクセス権があるかどうかを検証します。
- ほとんどの場合、ユーザーの資格は別の安全なコンテナ形式（通常EMM、資格管理メッセージとも呼ばれる）でカプセル化されており、ブロードキャスト配信ネットワークを介してプッシュ配信されるため、受信側の消費者デバイスは、スマートカードまたは他の安全なストレージを使用して、ユーザーアクセス権のデータベースを取得、処理、および維持できます。

コネクテッドCAS

コネクテッドCASソリューションは、リモート・サーバーと双方向接続できるため、コンテンツへのアクセスを許可する前にサーバーは、少なくともビデオ・レンダリング・デバイスとユーザーの認証情報を確認できます。オプションとして、IPチャンネルを介して放送コンテンツと共にスクランブル解読キーを転送することもできます。コネクテッドCASソリューションは、片方向CASの実装に比べて、次のような利点を持っています。

- 受信デバイスに埋め込まれたセキュリティ・コンポネントのレベルおよび複雑さを大幅に軽減することができるため、通常、スマートカードを使用する必要がなく、コストを減らすことができます。
- レンダリング・デバイスを遠隔制御することができ、必要ならブラックリストに入れることができます。

デジタル著作権管理

初期にデジタル著作権管理ソリューションは、オンデマンドでエンド・ユーザーに配信されることが多い、映画や歌曲などのオーディオ/ビデオ資産（ほとんどの場合インターネット経由で配信されるファイル）を保護するように設計されていました。すべてのDRMには次のような共通点があります：

- 配信よりもかなり以前にあるいは配信の直前に、オフラインでオーディオ/ビデオ資産にスクランブルをかけて、サーバーに保存することができます。ほとんどの場合、スクランブリング・ステップは、MPEG-DASH ABRプロトコルなどを使用して、配信する資料を準備する、よりグローバルなパッケージング・プロセスの不可欠な要素です。
- レンダリング・デバイス（プレーヤー）からの要請に応じて、コンテンツの再生時にスクランブル解読キーを伝送します。スクランブル解読キーは、デバイスが認証され、上述のコンテンツへのアクセスを許可するための商取引が正常に完了した時にのみプレーヤー・デバイスに配信される固有のライセンス・ファイルに含まれています。

© Copyright 2018 Technicolor.2018年11月22日

最先端で安全なCAS実装

ハッキングを防止するために、あらゆるCASおよび/またはDRMソリューションの安全で将来性のある最先端の実装は、ビデオ・デバイス・メーカーがいくつかのセキュリティ・コンポーネントを適切に実装し、非常に要求の厳しいデバイスの認証、製造、フィールド・サポートのプロセスを熟知することを要求します。コンプライアンスおよび堅牢性の規則として知られているこのような期待は、各コンテンツ保護ソリューションのベンダーごとに異なり、次のように大別することができます。

コンテンツ保護技術統合をサポートする4つの柱

安全性が保証されたハードウェア

長年にわたり、CASソリューション・ベンダーは、CASソリューションのソフトウェア・コンポーネントをあらゆる種類の侵入から効率的に保護するために、ハードウェア設計要件を大幅に増やしてきました。

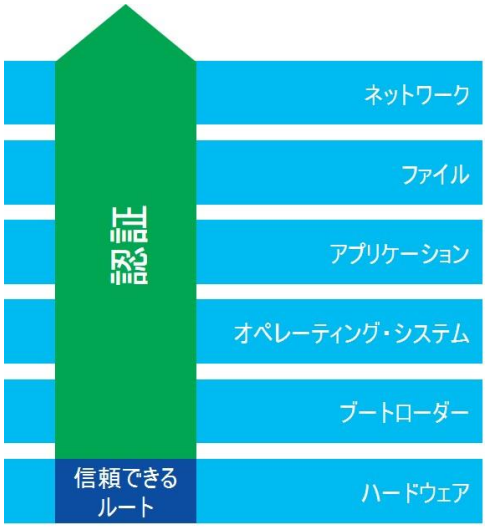
デバイス・メーカーが厳格に満たさなければならないハードウェア設計ガイドライン作ったCASソリューション・ベンダーは、追加のセキュリティ機能も定義しました。これらのセキュリティ機能は、主要なSoC（システムオンチップ）コンポーネントに次第に直接統合されました。その一例が、セキュア・ブートローダーと他の多くのセキュア・プロセスで使用されるキー・ラダーです。

各CASソリューション・ベンダーに固有のデバイス認証プロセスでは、これらの要件が完全順守されているかどうかを厳密に検証します。

安全性が保証されたブートローダー

コンテンツ保護を担当するソフトウェア・コンポーネントが、デバイスで同時に実行される可能性のある他のソフトウェア・コンポーネントやアプリケーションなどを介して改ざんされないようにするために、信頼できるハードウェア・ルートに基づいたセキュア・ブート・プロセスを実装しています。デバイスで実行されるすべてのソフトウェアは、実行前に認証過程を経ます。

多くの場合、セキュア・ブート・アーキテクチャは、CASソリューション・ベンダーによって規定され、デバイス製造時に統合するためにデバイス・メーカーに提供される一連のルート・キー（キー・ラダー）を利用します。あるいは、独立した第三者機関による認証が使用される場合もあります。



これらの認証要件はソフトウェア・アップグレード・システム（ダウンローダー）にも適用されるため、ライフサイクル中に追加のソフトウェア・コンポーネントとしてまたは既存のソフトウェア・コンポーネントに代わるものとしてデバイスにロードされる新しいソフトウェア・コンポーネントは、認証過程を経た後に保存されます。

© Copyright 2018 Technicolor 2018年11月22日

Android TVソフトウェアのサイズはかなり大きいため、ブートおよびローダーのアーキテクチャーは、ソフトウェア・モジュールの認証などのさまざまな面で、従来のLinuxの実装とは大きく異なります。

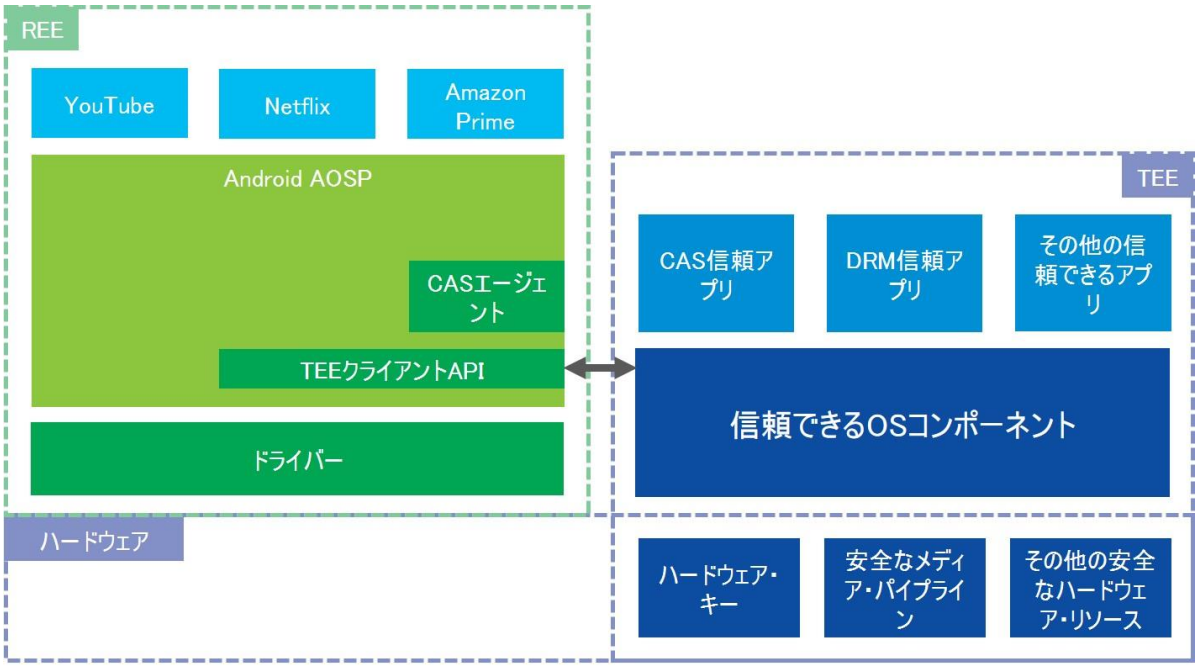
安全性が保証されたメディア・パイプライン

レンダリング・デバイスに配信されたデジタル・オーディオ／ビデオ・コンテンツは、まず圧縮した後に、スクランブルをかけます。受信デバイスでは、まずスクランブル解読を行った後にのみ、解凍を行えるため、いったんスクランブル解読が行われたコンテンツは違法コピーまたは再配布されやすいです。これを防止するためには、ハードウェアまたはソフトウェアの手段でコンテンツにアクセスできないように、メディア・パイプライン全体（スクランブル解読、解凍、グラフィック・プレーン・オーバーレイ、HDCP保護を含む安全なビデオ・パス）を実装する必要があります。スクランブル解読キーにもアクセスできないようにする必要があります。これにより、よく知られた著作権侵害技術（キー共有とも呼ばれる）を防止することができます。

信頼できる実行環境

下図の高レベル・アーキテクチャで示されている信頼できる実行環境（TEE）は、ハードウェア・メカニズムによって隔離されており、重要な操作を実行するように設計された認証済みのソフトウェア（信頼できるアプリケーション）のみを実行する安全な処理環境を提供します。

© Copyright 2018 Technicolor.2018年11月22日



REE 充実した実行環境

TEE 信頼できる実行環境

このような重要な操作としては、従来のCASソリューションのECMおよびEMMメッセージの処理と、コンテンツにあるスクランブル解読キーとユーザー権限を含んでいるDRMライセンスの処理があります。

この信頼できる実行環境のみは、ソフトウェアの認証に必要な重要なハードウェア・リソースと、安全なメディア・パイプラインの重要なハードウェア・リソースに直接アクセスでき、このようなアクセスは保護されています。

工程

消費者が家庭で利用する有料ビデオ・デバイスの平均寿命は7～10年以上です。従って、デバイス・メーカーは、すべての要件を完全順守する認定製品を設計・製造するためだけでなく、CASおよびDRMソリューション・ベンダーが制定したコンプライアンスおよび堅牢性の規則に従って有料ビデオ・サービス・プロバイダーに、展開されたデバイスを維持するのに必要なすべてのサポートをデバイスの寿命期間中に提供するためにも可能な全ての処置を取る必要があります。最も重要である、セキュリティ・ソリューションの再生能力は、さまざまな面で、デバイスの製造工程と販売後のサポートおよび保守に影響を与えます。

この目的を達成するために、テクニカラーのセキュリティー責任者が次のような工程と活動を直接監視しています。

デバイス認証

セットトップボックスを統合するデバイス・メーカーは、コンテンツ保護ソリューション・ベンダーが要求するコンプライアンスおよび堅牢性の規則を順守するために必要とされるCASおよび/またはDRMソリューションの実装に関して全責任を負います。この分野で30年間の経験があるテクニカラーは、他社より競争力がとても高いです。テクニカラーは、製品化までの時間を短縮し、総所有コストを下げることができます。

© Copyright 2018 Technicolor 2018年11月22日

デバイス製造

前述の統合および認証の規則を順守するために、デバイス製造工程では非常に多くの契約上の義務を履行する必要があります。従って、次のような工程を経て仕事をしなければなりません。

- プラットフォーム上でキーを処理および保存し、OTP（*1回しか書き込みができない*）フラッシュ・メモリー管理機能で装置を保護するために、工場ソフトウェアをレビューし、適切に更新するプラットフォーム・セキュリティ工学
- コンテンツ保護キーの作成/処理と配信
- 大量生産を開始する前の現地工場でのテストとキー提供の検証
- サードパーティの報告およびデータ収集プロセスの定義および監視

このような期待水準を満たすために、テクニカラーは、独自のツールと業界最高の専門技術を開発しました。

販売後のサポート

有料ビデオ事業者は、製品やサービスの故障などにより他社の製品やサービスに移行した消費者がいつかは自社が提供するデバイスを再び使用するようになることを期待しています。CAPEXを最大限に高めるということは、デバイスを修理調整して、他の顧客構内で再び利用できるということを意味します。この目的を達成するために、デバイス・メーカーは、専用ツール（デバイス・スクリーニング用ツールなど）を提供して、デバイスの修理調整中および修理調整後にもコンテンツ保護ソリューション・ベンダーが要求する規則を完全順守しなければなりません。

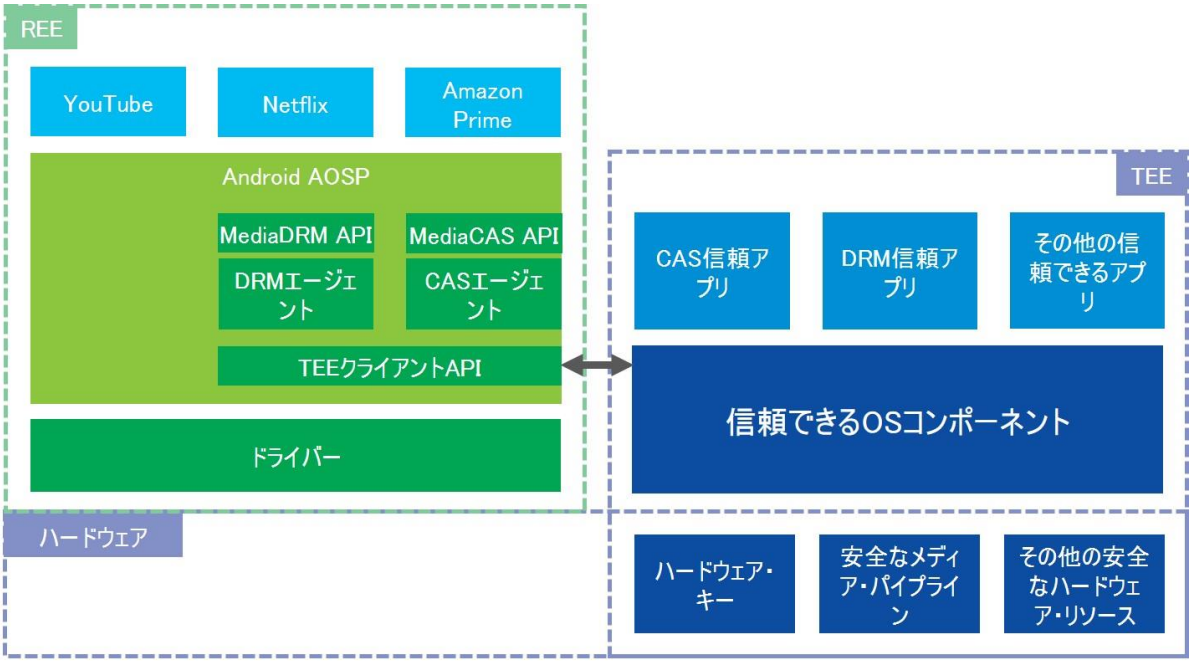
© Copyright 2018 Technicolor.2018年11月22日

CASはAndroid TVにどのように統合されていますか？

2014年にAndroid Lと共に発売されたAndroid TVでは、無料の線形テレビ・サービスの受信に対応するためにTIF（TV入力フレームワーク）を導入しましたが、有料のテレビ・サービスをサポートできるフレームワークはありませんでした。

最初のAndroid TVは超高解像度対応デバイスに展開されたので、前述のECP文書に記載されているコンテンツ著作権所有者の要求を満たすためには、デュアル・ライブラリのCASソリューションが必要でした。このアーキテクチャでは、CASソフトウェアの一部分（下図のCASエージェント）がAndroidフレームワーク自体に統合されています。これは、REE（充実した実行環境）とも呼ばれます。一方、CASソフトウェアの最も安全で重要な部分は、TEE（信頼できる実行環境）で実行される、信頼できるCASアプリケーションとして実装されています。利用可能な統合フレームワークがなかったため、AndroidペイTVデバイスは限定受信ソリューションのアドホック統合を必要としました。

Googleは、既存のMediaDRM APIモデルを利用して、MediaCASと呼ばれる新しいAPIの導入に取り組んできました。目標は、市販の限定受信ソリューションを統合するための標準フレームワークを提供することです。これにより、各メーカーの仕様に合わせて統合する必要がなくなります。しかし、MediaCAS APIを安定的かつ円滑に使用および展開できるシステムは、2018年8月にリリースされたAndroid Pだけです。以下に示すように、このMediaCAS APIは、Androidアプリケーション環境でCASエージェントの上層で機能します。また、テクニカラーは既にMediaCAS APIの統合に着手しました。



REE 充実した実行環境

TEE 信頼できる実行環境

今後数年間でMediaCAS APIを展開することで、使用するCASソリューションの種類に関係なく、事業者のカスタム・ランチャー・アプリケーションの統合が容易になり、その移植性が高まるでしょうが、安全な実装のためのすべての要件を満たし、前述のコンプライアンスおよび堅牢性の規則を完全順守しなければなりません。従って、デバイス・ベンダーは、適切な統合と認証のための十分な知識とスキルを習得する必要があります。

© Copyright 2018 Technicolor 2018年11月22日

© Copyright 2018 Technicolor.2018年11月22日

Android TV向けの市販用CAS統合の準備

初期からAndroid TV市場を主導しており、セットトップボックスの開発分野で5年以上の経験があるテクニカラーは、今まで30社の事業者と契約を締結しました。このような締結の半分は、統合型CASソリューションを備えたハイブリッド・デバイスに関連したものです。テクニカラーは、市販用の認定限定受信ソリューションを搭載したAndroid TVデバイスを発売した最初の企業です。Android TVの市場に最初に参入したこれらのCASパートナーは、製品およびサービスを開発・統合するために、非常に密接に協力しました。これにより、すべての関係者は豊富な経験を積みました。

テクニカラーと協力してAndroid TVにCASおよびDRMを統合した企業（既に統合を完了して製品・サービスを提供している企業または現在統合を行っている企業）：

- Nagra Connect Dual
- Verimatrix Ultra（IPTV、DVB、OTT）
- Irdeto Cloaked CA IFCP
- Widevine Level 1
- Playready SL3000
- Cisco/Synamedia Videoguard
- Viaccess Connected Sentinel

© Copyright 2018 Technicolor 2018年11月22日

覚えておくべき点

超高解像度テレビおよびビデオ・サービスの登場により、コンテンツの保護、作成、およびパッケージ化方法と消費者デバイスへの配信方法に対するコンテンツ著作権所有者の期待水準は高まりました。Android TVの急激な成長により市場が急速に発展しているが、限定受信ソリューションとデジタル著作権管理ソリューションの統合はますます複雑になっています。

線形およびオンデマンド型のビデオ配信サービスを提供するコンテンツ・プロバイダーとペイTV事業者のビジネスは依然として高品質で信頼性が高く将来性のあるハイブリッドの消費者デバイスに依存しているため、このようなコンテンツ保護ソリューションの統合を軽視してはいけません。これを達成するのに必要な経験、知識とスキルは、テクニカラーと、ペイTV STB業界の他の少数の大手会社だけが持っています。

急速に発展しているこれらの技術とソリューション、およびそれらの非常に高い成熟度についてよく知っているテクニカラーは、テクノロジー・アセスメントと、自社の知識と経験に基づいて急速に変化する市場で安全にコンテンツを供給するための最善の長期オプションに関する助言を提供する、事業者にとって信頼できるアドバイザーになることができました。

© Copyright 2018 Technicolor.2018年11月22日

テクニカラーは世界中に
事務所を持っています

1, Rue Jeanne d’Arc
92443 Issy-les-Moulineaux, France
電話：+33 (0)1 41 86 50 00
ファックス：+33 (0)1 41 86 56 15

technicolor.com

© Copyright 2018 Technicolor.著作権所有。参照されているすべての商号は、それぞれの会社のサービスマーク、商標、または登録商標です。仕様は予告なしに変更されることがあります。
WP-028-V01-1811