



CryptoGuard

– Protect your content –



# Protection du contenu de la télévision payante

- ➔ CAS - SYSTÈME D'ACCÈS CONDITIONNEL
- ➔ SMS - SYSTÈME DE GESTION DES ABONNÉS
- ➔ SOLUTIONS AVEC ET SANS CARTE
- ➔ ÉVOLUTIF POUR TOUTE TAILLE D'OPÉRATEUR
- ➔ DÉPLOIEMENT RENTABLE ET RAPIDE



# Excellence dans la protection des contenus de Pay-TV – Depuis 2007

## À propos de CryptoGuard

**CryptoGuard est un fournisseur mondial de protection de contenu de télévision payante telle que l'accès conditionnel (CAS) et la gestion des droits numériques (DRM) pour toutes les plateformes DVB, IPTV et OTT. Les solutions de CryptoGuard sont flexibles, évolutives, rentables et prennent en charge un modèle commercial attractif de "paiement au fur et à mesure de la croissance" », idéal pour toutes les tailles de réseau et d'opérateur.**

L'aventure réussie a commencé en 2007 lorsque CryptoGuard a été fondée en Suède et a lancé son CAS, adapté au marché suédois de la télévision par câble. En raison de l'arrêt de l'analogique, la réglementation obligeait les câblo-opérateurs à chiffrer leur contenu et de nombreux petits opérateurs étaient confrontés à de sérieuses inquiétudes car les alternatives CAS existantes étaient très coûteuses.

CryptoGuard CAS s'est avéré avoir le bon prix, un niveau de sécurité élevé et une évolutivité pour toute taille de réseau, ce qui a conduit 70 % des câblo-opérateurs suédois à utiliser CryptoGuard CAS en 2010. L'introduction réussie en Suède a conduit à l'expansion de CryptoGuard sur le marché international et à la poursuite du développement de ses produits pour répondre aux demandes des principaux opérateurs et diffuseurs du monde entier.

Aujourd'hui, les solutions de l'entreprise ont été déployées par plus de 250 opérateurs dans plus de 60 pays à travers le monde, et un certain nombre de chaînes de télévision nationales ont choisi CryptoGuard comme partenaire de sécurité. CryptoGuard est bien positionné avec des bureaux de vente sur trois continents et un vaste écosystème de partenaires apportant sur le marché des solutions de classe mondiale.

Ces dernières années, CryptoGuard a élargi son portefeuille de produits avec la solution OTT de bout en bout qui comprend tout le nécessaire pour mettre en place un service OTT - traitement et distribution des flux, système de gestion, protection du contenu DRM et applications des utilisateurs. Ce système rentable, rapidement installé et évolutif permet aux opérateurs de toutes tailles de démarrer leurs services OTT, même avec un faible nombre d'utilisateurs.



**2007**

Fondée à Luleå, en Suède  
Lancement de CryptoGuard CAS

**2010**

70 % des opérateurs de télévision par câble suédois utilisent CryptoGuard CAS

**2012**

Premier déploiement IPTV

**2014**

Bureau de vente au Pérou

**2009**

Siège social établi à Motala, Suède

**2011**

Bureau de vente en Inde  
Première exposition internationale (ANGACOM)

**2013**

Bureau de vente en Pologne



## Solution CAS & SMS

Choisir le bon système d'accès conditionnel (CAS) est essentiel pour garantir que seuls les abonnés payants ont accès au contenu et pour pouvoir obtenir du contenu premium auprès des fournisseurs de contenu. CryptoGuard CAS utilise une sécurité avancée et est constamment amélioré avec les dernières innovations en matière de cryptage, brouillage logicielle et de renforcement de la sécurité. CryptoGuard lutte également activement contre le piratage par le biais de l'Audiovisuel - Anti Piracy Alliance (AAPA). CryptoGuard CAS est idéal pour les opérateurs de toutes tailles et peut atteindre des millions d'abonnés. Il prend en charge n'importe quel modèle commercial et peut être étendu avec des services DRM et OTT.

## Sécurité avancée

CryptoGuard CAS utilise des modules de sécurité côté tête de réseau, avec le matériel le plus sécurisé. Du côté des STB et CAM, CryptoGuard CAS a toujours utilisé un couplage sécurisé avec une protection de liaison pour éviter le partage de mots de contrôle. CryptoGuard CAS utilise

une sécurité avancée intégrée aux microprocesseurs DVB des principaux fournisseurs de microprocesseurs pour les solutions sans carte et basées sur cartes à puce. En plus de stocker les secrets dans des chipsets hautement sécurisés, l'obscurcissement des logiciels et la technologie de cryptage la plus puissante sont utilisés pour éviter le clonage d'appareils ou toute autre menace de piratage.



Les cartes à puce CryptoGuard utilisent toujours les puces les plus sécurisées disponibles sur le marché. Ces puces sont certifiées EAL5+ de pointe et rigoureusement testées.

Core



FARNCOMBE SECURITY AUDIT	
Company	CRYPTOGUARD
Product	CRYPTOGUARD CAS
Date	MARCH 2020

CryptoGuard CAS a réalisé Farncombe Security Audit® approuvé par les Hollywood Studios

**2016**

Partenaire de mise en œuvre certifié Widevine "CWIP"

**2018**

Déploiements dans plus de 50 pays à travers le monde  
Prix Super Entreprise II

**2020**

Nouvel audit de sécurité Farncombe® CAS et DRM

**2022**

Lancement de CryptoGuard OTT

**2015**

CAS sans carte  
Audit de sécurité Farncombe®  
Membre de l'AAPA

**2017**

Premier déploiement OTT  
Prix Super Entreprise I

**2019**

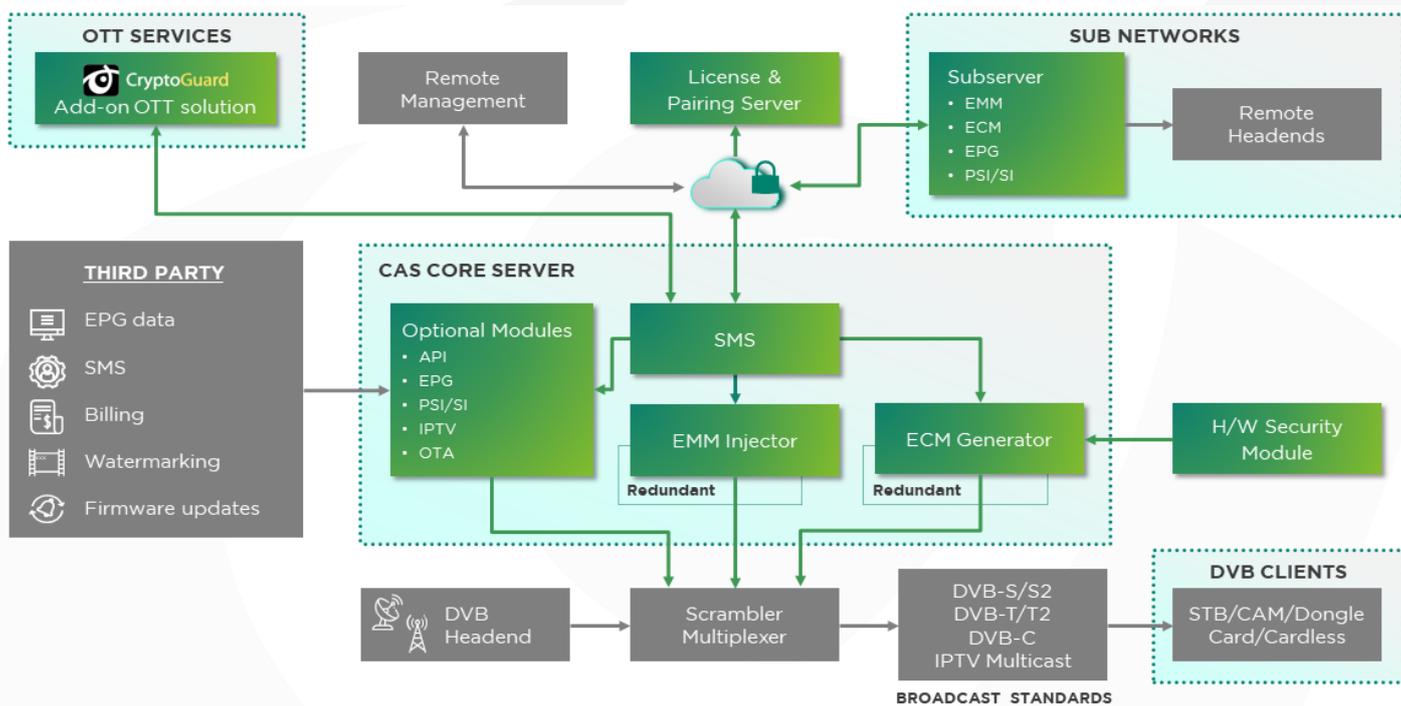
CAM sans carte  
Bureau de vente à Singapour  
Prix Super Entreprise III

**2021**

Déploiements par plus de 250 opérateurs dans plus de 60 pays à travers le monde

## Serveur Core

- ➔ CryptoGuard CAS peut exécuter toutes ses applications principales sur un seul serveur et peut facilement être étendu à de très grandes opérations en connectant davantage de sous-serveurs avec une redondance facultative.
- ➔ CryptoGuard CAS peut être configuré pour prendre en charge n'importe quelle topologie de réseau.
- ➔ Un serveur central CryptoGuard CAS Core peut contrôler de nombreux générateurs ECM et injecteurs EMM placés à différents endroits. Ainsi, les réseaux câblés situés dans différents endroits ou différentes liaisons montantes par satellite peuvent être exploités de manière centralisée comme un seul système à partir d'un seul serveur CryptoGuard CAS Core.



## Modules optionnels

- ➔ **API** - Pour l'intégration de systèmes tiers
- ➔ **EPG** - Collecte et envoie des données EPG aux utilisateurs. Le module EPG peut être utilisé dans un sous-serveur ou comme unité séparée dans n'importe quel réseau DVB. Le module EPG est également disponible pour le serveur EPG autonome pour les têtes de réseau CATV avec prise en charge des normes DVB et ISDB-Tb (Brésil).
- ➔ **IPTV** - Pour un système DVB-IPTV rentable. Fournit un CAS et une liste EPG/chaîne de Intergiciel de base aux STB IPTV.
- ➔ **PSI/SI** - Configurez les chaînes de télévision, par ex. sous-réseaux où les têtes de réseau locales sont utilisées avec une configuration différente. Génère et insère des tableaux NIT, SDT, SDT autres, TDT, TOT, CAT, PAT, BAT et EIT pour la configuration des listes de chaînes, des tableaux de fréquences et du guide des programmes (EPG).
- ➔ **OTA Player** - Permet la mise à niveau du micrologiciel "Over-The-Air" des décodeurs, des modules CA et des dongles.

## SMS – Interface Web pour le contrôle de CAS/DRM et OTT

Le SMS vous permet de gérer les abonnés, les appareils clients, le contenu, les commandes, le service client, la facturation, etc. L'architecture est ouverte, basée sur une base de données MySQL et Linux, et un ensemble complet d'API est disponible pour l'intégration avec des systèmes tiers. CryptoGuard CAS peut être étendu avec la solution CryptoGuard OTT et la sécurité DRM. Tous les abonnés DVB/OTT et les appareils clients sont gérés de manière transparente via le serveur Core CAS.

### CAS

- ➔ Gestion des sous-serveurs et des redondances
- ➔ Gestion des abonnés et contenu
- ➔ Gestion des appareils clients, STB, CAM et dongles
- ➔ Prise d'empreintes digitales EMM et ECM
- ➔ Réglage de force STB et messagerie
- ➔ Paramètres du module : API, PSI/SI, EPG, OTA et IPTV

### Système OTT et DRM

- ➔ Gestion des redondances
- ➔ Gestion des abonnés et contenu
- ➔ Gestion des appareils clients : Mobiles, PC, SmartTV et STB
- ➔ Paramètres DRM : droits de contenu, nombre d'appareils, restrictions géographiques

### Aperçu du menu SMS

Customers/Devices	Access criterias	Products	Reports	Configuration
Manage customers	Manage access criterias	Channel packages	Activation history	Backup
Manage devices	Manage access criteria profile	Services	Active devices	EMM fingerprinting
Advanced search	PPV programs	Customer groups	Broadcaster report	EMM OTA trigger
Reseller customer form	PPV program manager	Articles	Card statistics	Force tuning
File import		Manage price changes	Card versions	IP setup
		Reseller package group names	Channel statistics	Manage networks
		Broadcasters	Customer definition channel stat's	Messages
			EMM statistics	Multicast EMM
			Ended subscriptions	OTA Player
			Generate card numbers	PDF contract template
			Inactive customers	Process control
			Invoice list	Router setup
			Message queues	Simulcrypt ECM
			Package statistics	Simulcrypt EMM
			Paired STB's	System setup
			PPV order history	
			Subscriber list	
			Valid subscriptions	

PSI/SI insert	Log files	DRM/OTT	Administration
EIT containers	Alarm log	Encryptor services	Manage users
IPTV channel list	System log	Geo filters	Manage roles
PSI/SI	User log	Stream profiles	IP access list
	IP EMM log	Assets	

### Sous-réseau

- ➔ Ayant des réseaux étendus sur une zone géographique plus vaste avec des tables de fréquences différentes ou disposant de plusieurs têtes de réseau, il peut être nécessaire d'utiliser des composants distincts du serveur principal. Un exemple est un serveur supplémentaire PSI/SI, ECM ou EMM.
- ➔ Le module EPG peut être installé séparément sur un sous-serveur et peut également être utilisé comme serveur EPG autonome dans les têtes de réseau TV prenant en charge les normes DVB et ISDB-Tb (Brésil).

## Redondance

- ➔ CryptoGuard CAS peut être configuré pour prendre en charge n'importe quelle topologie de réseau et un serveur CAS central peut contrôler de nombreux générateurs ECM et injecteurs EMM (sous-serveurs CryptoGuard).
- ➔ Le générateur ECM peut être séparé du serveur principal et installé sur un sous-serveur, qui communique avec le serveur principal. Cela peut être fait pour améliorer les performances, puisque la génération ECM est la partie la plus lourde et la plus sensible d'un système CAS.
- ➔ Un deuxième serveur ECM peut également être installé pour des raisons de redondance, le brouilleur de tête de réseau détectant si un serveur ECM tombe en panne, pour se connecter automatiquement au deuxième.
- ➔ EMM peut également être installé sur un sous-serveur distinct pour alléger la charge du serveur principal
- ➔ Avec ce concept, il est possible d'ajouter plusieurs sous-serveurs CryptoGuard pour obtenir les performances nécessaires. En ajoutant davantage de serveurs principaux CryptoGuard CAS et de sous-serveurs Crypto-Guard, CryptoGuard CAS peut s'adapter à un très grand nombre d'abonnés.



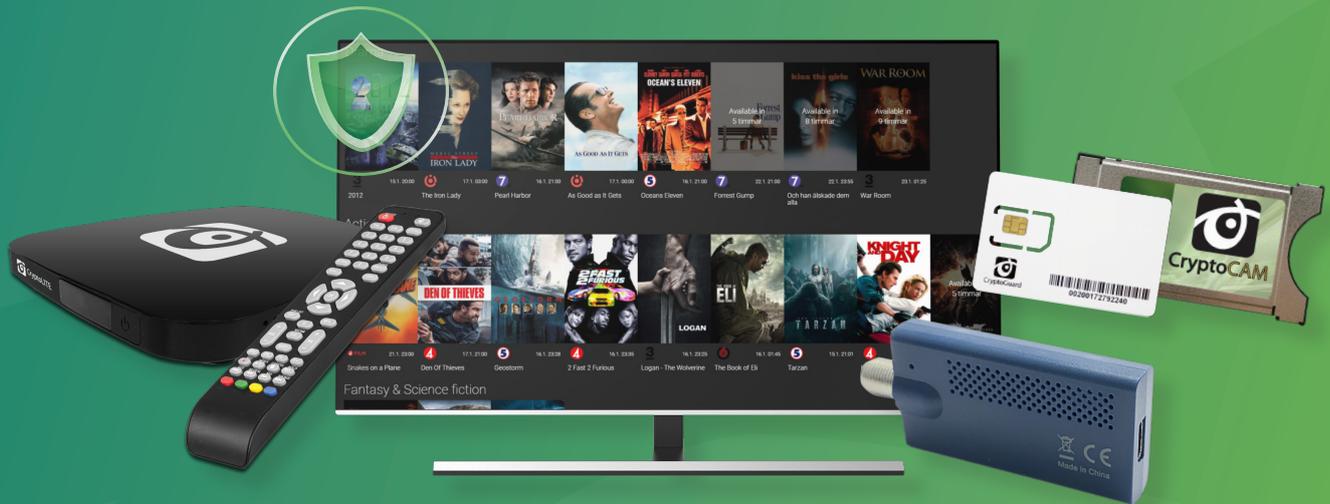
## Solution hybride DVB et OTT Pay-TV

- ➔ CryptoGuard CAS peut également être étendu avec la solution économique CryptoGuard OTT de bout en bout contenant un serveur OTT, un transcodeur, un serveur Origin, des serveurs CDN et des applications pour iOS, Android, Smart TV et STB.
- ➔ La solution CryptoGuard OTT comprend également CryptoGuard DRM grâce auquel l'opérateur de télévision payante peut gérer le contenu et les abonnés à partir du serveur principal CAS.
- ➔ CryptoGuard DRM prend en charge les formats les plus populaires Widevine, FairPlay et PlayReady, permettant une diffusion de contenu hautement sécurisée. Ces DRM sont nativement pris en charge par la majorité des appareils clients et sont approuvés par les grands studios.

## Caractéristiques Techniques

Nombre d'abonnés pris en charge	N'importe quelle taille, pratiquement illimitée
Modèles commerciaux pris en charge	Abonnement, Pay Per View et événements
Transmission prise en charge	DVB-C, DVB-T/T2, DVB-S/S2, IPTV
Prise en charge multi-réseau	Un serveur CryptoGuard CAS peut prendre en charge de nombreux sous-serveurs
Prise en charge multi-opérateurs	Un serveur CryptoGuard CAS peut servir de nombreux opérateurs
Version simulcrypt	ETSI TS 103 197 V 1.2.1 and V 1.3.1 (Simulcrypt 2 and 3)
Système de gestion des abonnés, SMS	Un SMS pour contrôler les abonnés dans le système CryptoGuard CAS est inclus
API pour la facturation / SMS tiers	Oui
Contrôle sans carte et carte à puce	Client, propriétaire de réseau, fournisseur de programmes
Ventes d'abonnements	Service client, connexion abonné avec code PIN, codes d'activation prépayés, connexion revendeur
PPV et VOD	Oui
DRM	Oui, pris en charge via CryptoGuard DRM
Prise en charge multi-DRM	Google Widevine, Apple FairPlay et Microsoft PlayReady
Technologie d'activation	Balises et numéros de programme. Dernière date de péremption, contrôle positif et contrôle négatif
Base de données et redondance	MariaDB (anciennement MySQL) prend en charge le cluster maître-esclave et Galera
Les privilèges d'administrateur	L'accès au système peut être défini par utilisateur et des rôles personnalisés peuvent être créés
PSI/SI-play out	NIT, SDT, SDT actual/other, CAT, TDT, TOT, Private Sections
Serveurs pris en charge	Intel 64 bits, 8G de Ram et 400G de disque. Diverses têtes de réseau et Raspberry Pi pour les petits réseaux
CAM Soutien	CAM pour CI et CI+. CAM professionnelles pour 4, 8, ou 16 services
Pairing	Oui, à la fois sur la sécurité standard et avancée, contrôlée au niveau du canal
Control word sharing protection	Oiu, on both Standard and Advanced Security
# Channels/channel package/MUX	Unlimited, defined on order. Standard is 512 tags. Several channels can have the same tag
STB pris en charge	Une liste distincte des STB testés est disponible
Over the Air mise à niveau des STB	Oui, pris en charge à la fois pour le middleware STB et le client CryptoGuard Cardless CAS
Mise à jour/nouvelles versions	Tous les opérateurs disposant d'un SLA actif bénéficieront en permanence de mises à niveau de serveur.
Messages texte aux utilisateurs	Messages jusqu'à 2048 caractères
Fingerprinting	Group, individual, set position and moving position
Forced tuning	Yes
Rapports	Rapports standards et personnalisés
Installation rapide	Oui, via le kick starter
OTT	Oui, CryptoGuard OTT prend en charge la solution OTT complète de bout en bout

# Appareils clients CryptoGuard CAS:



CryptoGuard dispose d'un vaste écosystème de partenaires et propose une large gamme d'appareils clients avec et sans carte:

## Décodeur numérique

- ➔ Avec et sans carte
- ➔ DVB-S/S2, DVB-T/T2, DVB-C, DVB-IPTV
- ➔ Zappers, DVB Hybrid, DVB/Android
- ➔ SD, HD, MPEG-2, MPEG-4, HEVC

## Module CA

- ➔ Avec et sans carte
- ➔ CAM professionnelle jusqu'à 16 services

## Clé de télévision payante

- ➔ Ajoute des chaînes DVB Pay-TV aux appareils mobiles Android ou aux décodeurs



Lire la suite ici:

[www.cryptoguard.com](http://www.cryptoguard.com)

CryptoGuard est un fournisseur mondial de solutions de protection de contenu de télévision payante telles que l'accès conditionnel (CAS) et la gestion des droits numériques (DRM) ainsi que des solutions IPTV/OTT de bout en bout.

CryptoGuard AB  
Östermalmsgatan 101  
SE-591 60 MOTALA  
Sweden

Tel: +46 971 107 35  
[sales@cryptoguard.com](mailto:sales@cryptoguard.com)  
[www.cryptoguard.com](http://www.cryptoguard.com)

