



Conditional Access-Lösungen für digitales Fernsehen

Michael Schacht, Geschäftsführer, Conax GmbH

Cable Days 2007 – Fachtagung am 18./19. Oktober 2007

www.conax.com

Conax - Ein erfolgreicher CA Anbieter



Kernleistung: Zuverlässige und innovative Inhalte-Sicherheit für die digitale Fernseh-Verbreitung

- Conax gehört zu 100% zu Telenor Broadcast
- Mehr als 200 Kunden in über 70 Ländern
- Millionen Smartcards verbreitet – > 15 Mio. 2007
- Schnellst wachsender CA Anbieter 2003 - 2007
- Firmensitz in Oslo
- Tochtergesellschaften in Deutschland, Indien und den USA
- Büros in Singapore, China, Brasilien, Korea, Russland und Kanada

Weitere Leistungsfelder:

- On-Demand services
- IPTV
- Digital Rights Management (DRM)
- Mobile TV



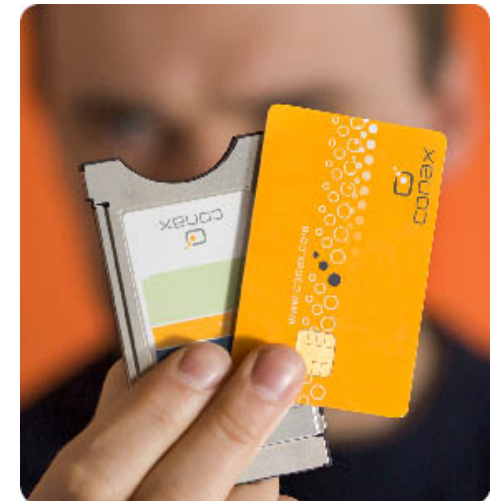
Conax - Die Kernleistung



Langfristige Sicherheit durch smartcard-basierte CA-Lösung - für alle broadcast and IP services geeignet

- Hardware-basierte Sicherheits-Grundlage
- Präventive Abwehr von Hacker-Angriffen
- Conax CAS7 als aktuelles System
- Weitgehend skalierbar und kosten-effezient
- Für kleine und große Netze
- Geeignet für DVB Broadcast und IPTV
- Sicherheit für VoD und PushVoD

“Conax main focus is to help its customers to create new business opportunities”



- Conditional Access: Werkzeug und Service – nicht “Kosten” ...
- Mit dem “richtigen” CAS Aufwand für System-Komponenten und *operative Kosten reduzieren*

Maximale Kompatibilität



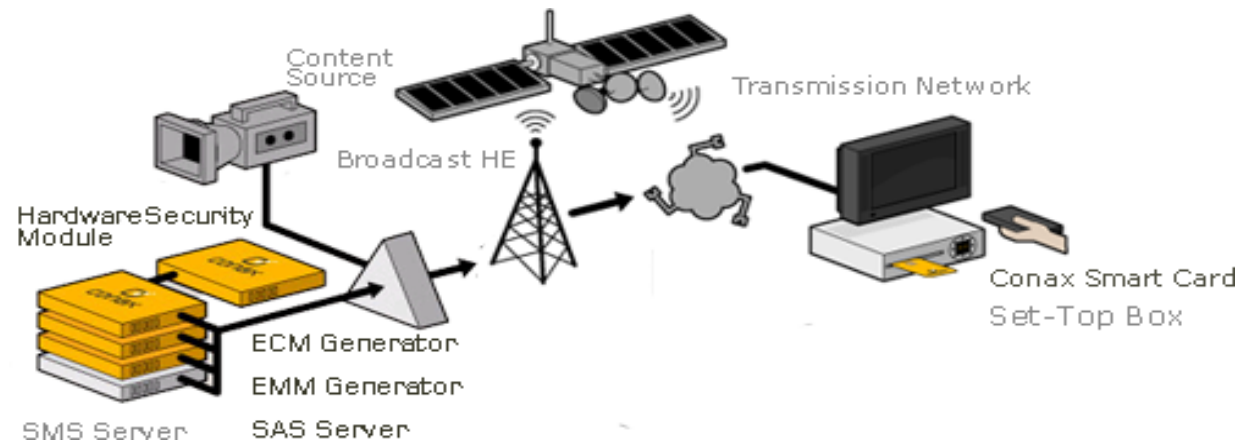
- Interoperabilität als Anforderung
- Maximale DVB Konformität
- DVB Simulcrypt kompatibel
- Interoperabel in jeder Play-out Umgebung
- Kooperation mit System-Integratoren, überall dort, wo die Komponenten weiterer Hersteller integriert werden
- Bedient alle Rückkanäle: Kabelmodem, IVR, GSM/SMS, etc.
- Definiertes Interface zum SMS-System – egal welches
- Volle Integration mit MHP und weiteren Middleware-Systemen
- Standard Definition und High Definition
- Auswahl unter mehr als 250 Set Top Boxen
- Aktive Unterstützung von Multicrypt-Implementationen

Conax CAS7: Core



Pay-TV im Abonnement - über einen definierten Zeitraum

- **Conax CAS7 SAS Server** Adressierung/Freischaltung der Smartcards (EMMs)
- **Conax CAS7 EMM Injector** Play-out/Übertragung der EMMs zum Multiplexer
- **Conax CAS7 ECM Generator** Enkodierung/Autorisierung der verschlüsselten Programme
- **Conax Smartcard** erkennt EMMs/ECMs und schaltet die abonnierten Programme frei



Conax CAS7: Weitere Module



Erweitertes Leistungsangebot

- **Conax CAS7 Event PPV/NVOD** Individuelle Adressierung einzelner Programme
- **Conax CAS7 IP** Sichere on-demand und IPTV Verbreitung auf jedem Netz
- **Conax CAS7 VOD** Adressierung einzelner Programme auf Abruf; „on-the-fly“, „push“, à la Carte und „time-shiftTV“
- **Conax CAS7 Watermarking und Fingerprinting** Quell-Erkennung unrechtmäßig verbreiteter Programmkopien

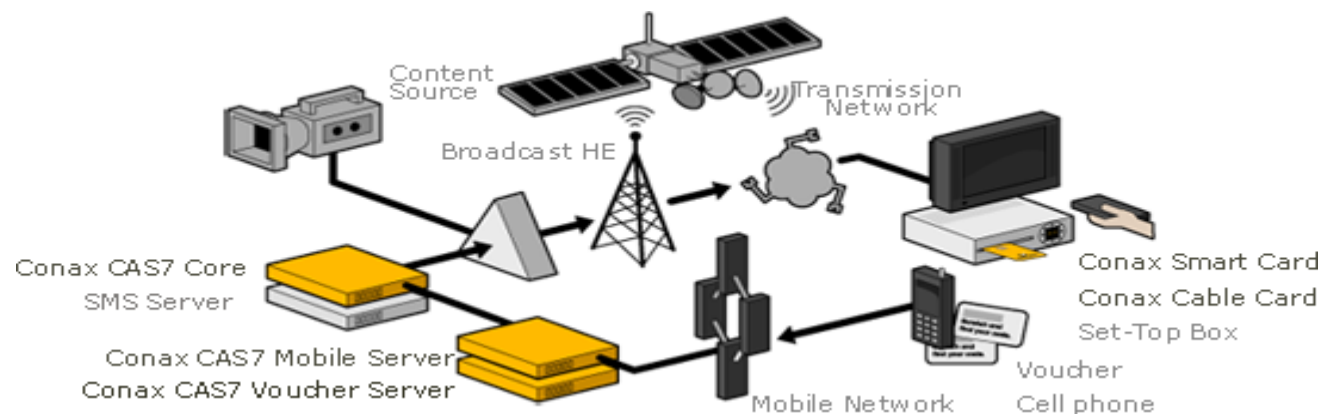


Conax CAS7: Mehr Werkzeuge



Systemkomponenten und Prozess-Unterstützung

- **Conax CAS7 Mobile Server** Bestellungen für PPV- und „prepaid“ Abonnements über mobile Textnachrichten (SMS)
- **Conax CAS7 Tokens PPV und Voucher Server** Vorausbezahlte pay-per-view-Adressierung
- **Conax CAS7 Messaging** Individuelle und gruppen-adressierte Textnachrichten an Smartcards und STBen
- **Conax CAS7 Data Playout Manager** System-Software-download auf STBen



Conax CAS7: IP



- **Eine** CAS-Installation für die DVB- und IP-Verbreitung
- Eine Smartcard für alle Services
- Encryption und Rechte-Management (ECM, EMM) auf MPEG2-Transportstrom-Ebene (MPEG2-TS), dem Träger für die Audio- und Video-Übertragung
- Daher: für alle MPEG2/MPEG4/H.264/AVC Kompressions- und Encoding Verfahren verwendbar

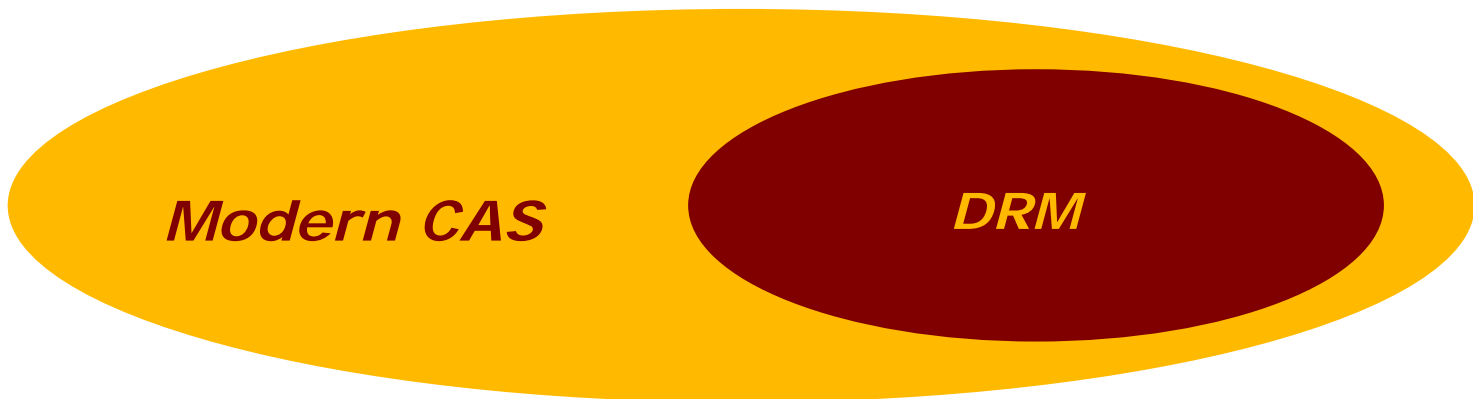
	Content in ES packetised format, e.g. MPEG2, 3, 4, VC1, AC3, etc	Content in ES packetised format, e.g. MPEG2, 3, 4, VC1, AC3, etc	Content in ES packetised format, e.g. MPEG2, 3, 4, VC1, AC3, etc
Conax CAS 7 acts on this layer, using CSA	MPEG-2 TS	MPEG-2 TS	MPEG-2 TS
	FEC	RTP	Viterbi
	4 or 8 PSK	UDP	X QAM
	Satellite link	IP	COFDM
		PHY	Terrestrial link
	DVB S, S2	IPTV	DTT

DRM: Was das CAS leistet



CAS oder DRM ?

- **DRM-Funktionen sind Teil des CAS**
- EMMs autorisieren Einzelne Adressaten oder ganze Gruppen (Entitlement = Right; EMM ist im Kern eine DRM Nachricht)
- ECMs beschreiben Inhalte, die bestimmte Berechtigungen erfordern
- Beispiele für "Berechtigungen": HD-Empfang oder nicht, Aufzeichnung auf Festplatte oder nicht, aufzeichnen und 24 Stunden nutzen, kopieren, auf andere Geräte überspielen etc., wie mit DRM



Herkömmliches DRMS vs. CAS



Zusammenarbeit mit Microsoft

- Microsoft als Marktführer bei traditionellen DRM-Systemen:
 - DRM für PCs
 - Nicht kompatibel mit DVB
 - Schwächer als CAS
 - DRM: 1 key per movie
 - CAS: 1 key per 10 seconds
- Conax als CAS-Experte:
 - DRM für Set Top Boxen
- Microsoft und Conax führen zusammen: Conax CAS und klassische DRM-Funktionen aus der PC-Umgebung

Watermarking und Fingerprinting



Conax bietet Inhalte-Schutz in 3 Schritten

- CAS: Autorisierung von Empfang – Ja oder Nein ?
- DRM: Was der Abonnent mit dem Inhalt tun darf, und auf welchen Geräten ?
- Fingerprinting und Watermarking: Im Fall von illegalen Kopien die Verfolgung des Piraten

- Fingerprinting und Watermarking hinterlassen "Spuren" im dekodierten Video
- Eindeutige Bezeichnung des Ursprungs (STB oder Smart card)
- Fingerprinting: Sichtbar (nicht einfach); schwach, aber in den meisten Fällen ausreichend
- Watermarking: Unsichtbar, nicht auffindbar; stärker

Conax VoD und Push VoD

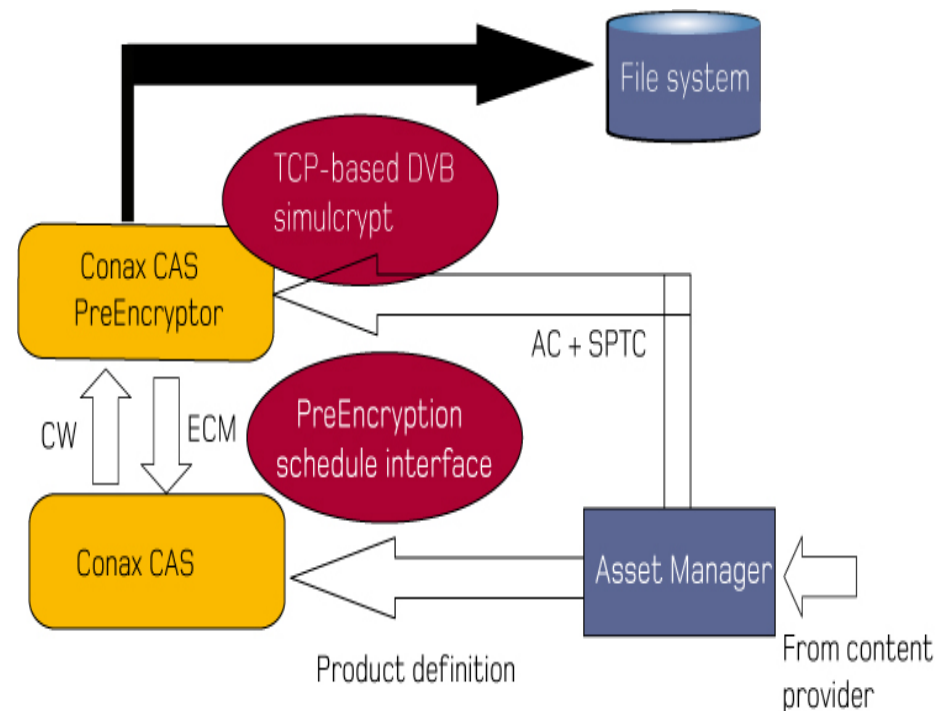


- Broadcast TV als Grundlage des digitalen Kundengeschäftes
- Ein integriertes Sicherheitssystem für Broadcast und On- Demand Services gleichzeitig
- Conax VOD:
 - Vorverschlüsselt (pre-scrambled) oder session based;
 - Trick Modes unterstützt (fast forward, rewind, pause);
 - Alle Geschäftsmodelle:
Subscription VOD; time-shift TV
Nutzung für bestimmte Zeiträume, à la carte, etc.
 - Integration mit einer Vielzahl von Server-Herstellern realisiert
- Conax Push VOD:
 - Download von Filmen auf Personal Video Recorder (SD/HD) und Ferbedienung der Aufzeichnungen/Festplatte
 - Konsument kauft die Filme von seiner Festplatte, z.B. Über sein Mobiltelefon (SMS)
 - Von verschiedenen Betreibern heute angeboten

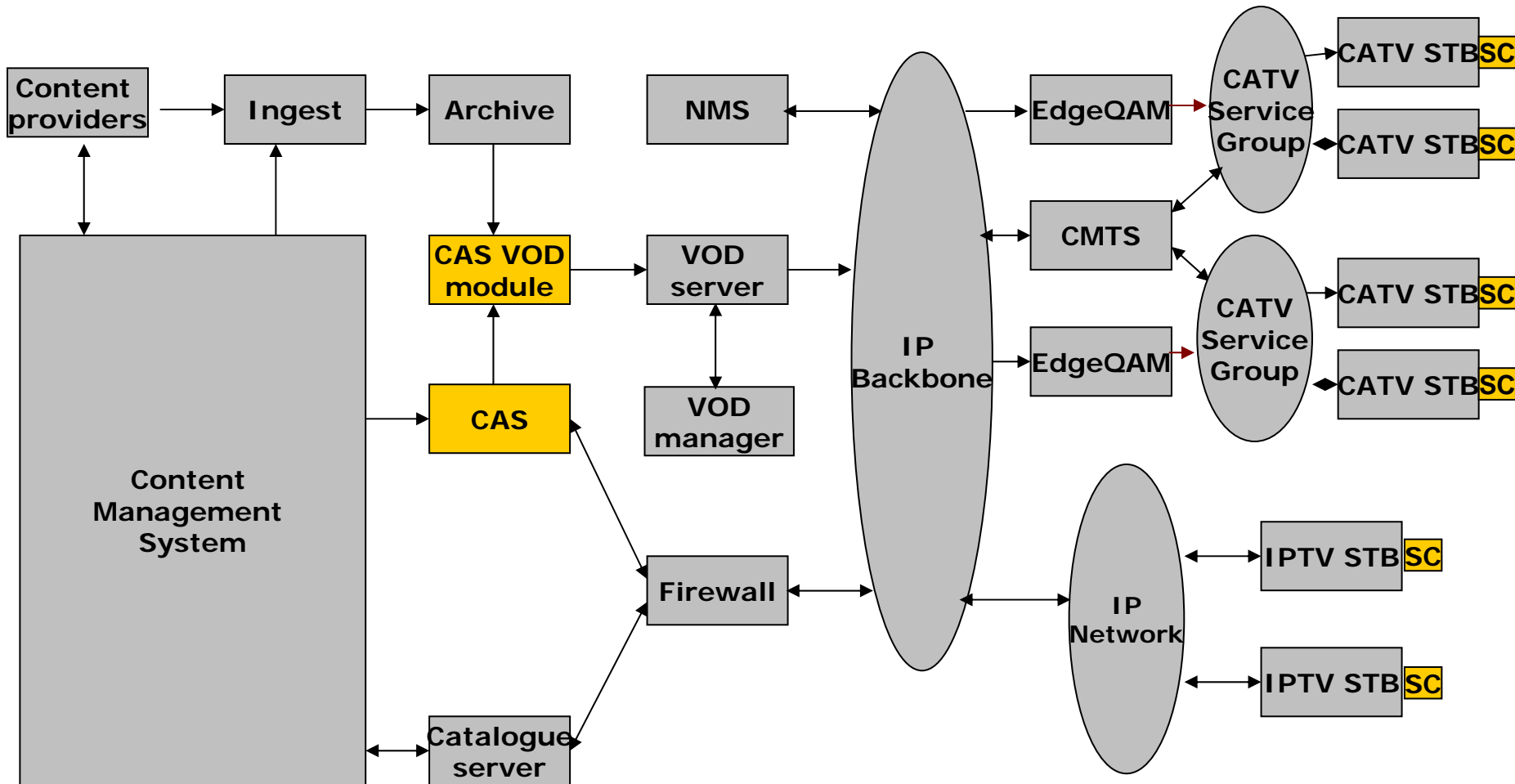
Conax VoD-Lösungen



- Derselbe hohe Sicherheitsstandard für alle VoD und broadcast Services
- Conax bietet alle "CA and DRM Services"-Komponenten:
 - Copy-protection durch scrambling
 - Access control durch Smartcard
 - Autorisierung der Kunden
 - Beleg bei Nicht-Anerkennung von Bestellungen (Signatur der Bestellung durch die Smart Card)
- Chipset pairing verpflichtend für die Implementierung von Conax VoD oder pushVoD in STBen



Beispiel eines VOD-Systems 1



Beispiel eines VoD-Systems 2



Conax stellt bereit:

- **Sicherheits-Komponenten** für VoD und pushVoD als zusätzliche Module zu Conax CAS7 Core, z.B.
 - Den Pre-encryptor
 - Das On-demand Entitlement Gateway
- **Integrations-Richtlinien** und Support für VOD Server-Hersteller und System-Integratoren
 - Beschreibung von Interfaces, message flows etc. mit den technischen Details
- **VoD-Integrations-Baukasten für STB-Hersteller**

Conax unterstützt:

- **Eine Vielzahl von Kauf- und Bezahl-Modellen**
- **Der Betreiber hat die Wahl** bei Content Management, VoD-Server, Rückkanal, Middleware and STB

Integration:

- Der Betreiber/sein Integrationspartner besorgen die Integration

CA-Sicherheit und STB-Lizenz



- Offene STB Politik
- Standard STBen unter Standard-Lizenz
- Weder Abgaben per STB noch Voraus-Entgelte
- **“Konformitäts-Test”** empfohlen
- Konformitäts-Test prüft die CA-bezogenen Basis-Funktionen der STB; Smartcard interface und management, Broadcast Prozesse, user interface etc.
- STB Pairing Lizenz: Mandatory **“security test”** zur Einordnung der STB in Sicherheitskatagorie; Konformitäts-Test inklusive; gegen Lizenzentgelt
- Tests werden von Conax oder zertifizierten Partnern ausgeführt



... System Software Updates



CA System und CA Lieferanten ersetzen können !

- Voraussetzungen:
 - Symulcrypt (DVB)-konformes CAS
 - Vertragliche Gewährleistung von Simulcrypt
 - Geeignete STBen (CSA, Standard Smartcardleser)
 - Verfügung über die "Schlüssel"
- STB akzeptiert den SSU Austausch und upgrade nur bei "richtigem" Private Key
- Wer den Private Key hat, beherrscht die STBen; dies gilt für **alle System Software**, nicht nur CA Software
- Software Download muss sicher sein ! Aber soll der CA-Lieferant die Kontrolle darüber haben ?



Thank you !

Conax GmbH
Charlottenstr. 68
D-10117 Berlin

Tel: 030 - 201 88 332
Fax: 030 - 201 88 333

www.conax.com
michael.schacht@conax.com