

Conditional Access & The Pay TV Environment

Bertrand WENDLING (Nagravision)

16 January 2009



Digital
Interoperability
Forum

- Who is DIF?
- Evolution of content distribution
- Opportunities and threats in digital distribution
- Overview Conditional Access
 - How CA works
 - The role of CA in the Pay TV environment
 - How is CA attacked
- Response to Piracy
- Summary

Who is DIF?

- **The Digital Interoperability Forum (DIF) is committed to delivering digital TV to Europe's citizens and fostering interoperable solutions for Digital TV.**
- **DIF's membership includes many of the leading companies in the delivery of digital TV in Europe:**
 - *Broadcasters: BSkyB, CANAL+, Liberty Global, Premiere, Sky Italia, TF1.*
 - *Operators: Arqiva, Deutsche Telekom.*
 - *Technology Suppliers: Microsoft, Nagravision, NDS, Qualcomm, Pace Micro Technology, Viaccess, ZetaCast.*
- **Members of DIF have driven the advance of digital TV in Europe:**
 - *Collective investment of billions of Euro.*
 - *Set technical standards.*
 - *Make digital TV a reality on many platforms.*

Evolution of content distribution

- **Pre 1980's: analogue content, physical distribution**

- *Audio cassette tapes, VCR, TV, paperback books.*
- *Distribution of content over physical channels (record shops, rental stores, cinemas).*



- **1980's - 1990's: digital content, physical distribution**

- *Digital content now more widely available (CDs, DVDs).*
- *Content is fully transitioning to digital (Digital TV, e-books, MP3, etc).*
- *As of late 1990's, digital content still distributed over physical channels (shops, rental stores).*



- **Today: digital content, digital distribution**

- *Many digital channels now available to distribute digital content (internet stores, digital TV, games distribution).*
- *Digital distribution is new and yet to come of age.*



■ New opportunities with Digital Distribution:

- *For content creators (reach new audiences, create new forms of content).*
- *For operators (new products, new revenue, interactivity).*
- *For users (personalized services, services on demand, portable devices).*

■ Threats to content in the Digital world:

- ***Digital copies are perfect copies of the original*** (the millionth copy is as good as the original).
- ***Digital packaging & distribution is easier than ever*** (there is a small studio in every home: PCs, high-capacity media, high-speed networks, Internet).
- ***Converging networks*** (hack one network, get three services: Internet / video / telephony).

The need to protect content in the digital world will continue to exist.

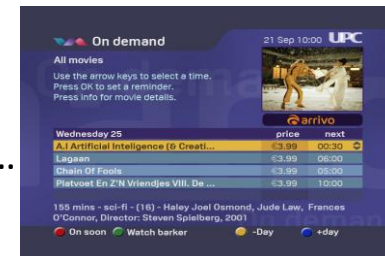
Overview of Conditional Access

What is CA?

- A technical system that controls who can watch broadcast content (e.g. TV).
- CA for broadcast TV **via conventional broadcast networks** is based on DVB standards which are industry-led technical solutions.
- CA solutions are provided by many different companies (e.g. Nagra, NDS, Viaccess, etc...).
- Interoperability of different CA solutions is possible presuming this is required by the business models involved, **but without mandating full standardization that prevents a quick reaction to piracy.**
- In short, CA provides access to content which is conditional to certain requirements (e.g. "Has service been requested?" "Has service been paid?").

What types of services are offered via CA?

- Basic broadcast TV services.
- Premium content such as movie, sport channels, video on demand.
- Interactive TV: email, video games, quiz shows, votes, betting, shopping...

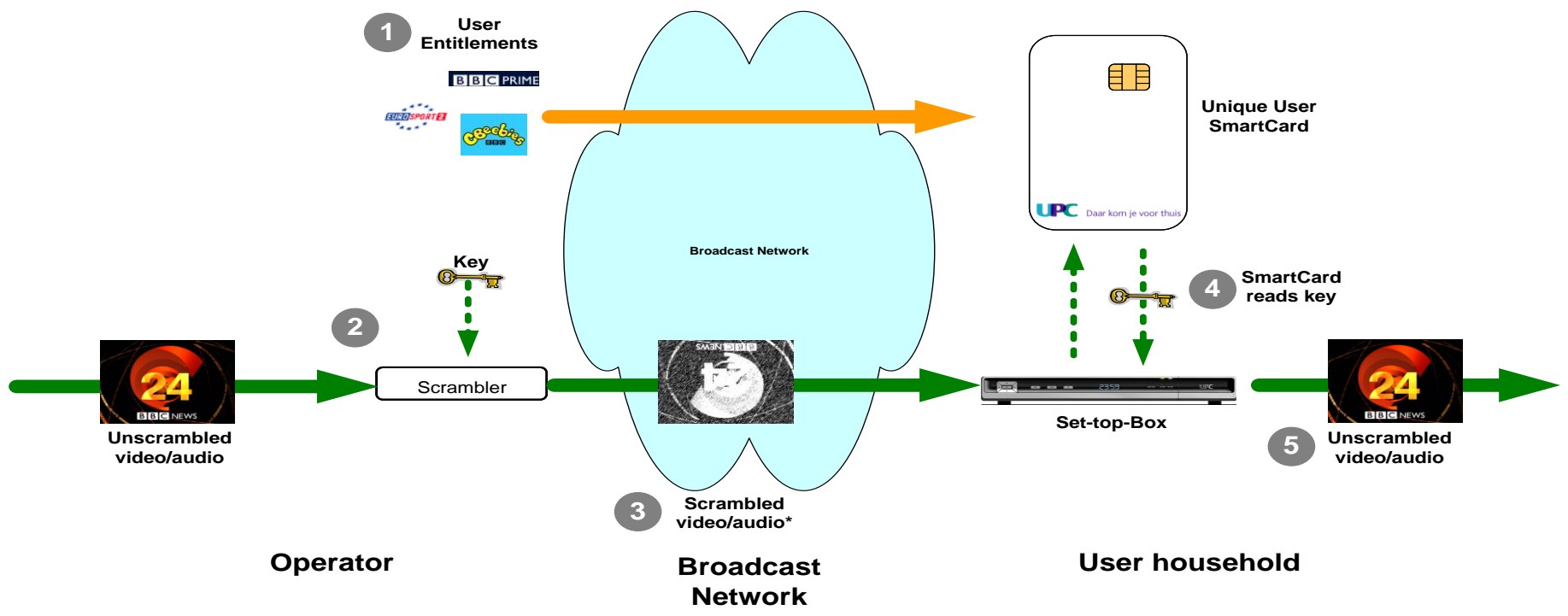


Why do broadcast providers use CA?

- To arrange thematically and personalize content & services.
- To fulfill their obligations of licensing rights and child protection.
- To provide interactivity.
- To Ensure that access to content is limited to customers who have paid for that content!



How Conditional Access works



The role of CA in the Pay TV environment

The importance of CA for the Pay TV environment

- *CA has allowed the emergence of new business models.*
- *CA allows choice:*
 - *content can be arranged thematically or “personalized” according to individual tastes (e.g. premium sports or movie content).*
- *This in turn saw a massive increase in the number of channels and type of content offered.*
- *Use of CA means that broadcasters and/or platform providers can extract reasonable return on investment for purchase and offer of this content (e.g. network upgrades; purchase of (exclusive) content premium rights).*
- *Which ultimately ensures right holders remunerated for premium content offered.*

The importance of Pay TV in the Audiovisual sector across Europe

- *Pay TV viewed by many as the precursor to digital TV as it created an appetite for more choice and control over TV services being offered.*
- *Pay TV will continue to play a pivotal role in the Audiovisual sector since premium content will always be in demand.*
- *As such the role of CA in the digital world is set to continue.*

The importance of CA in safeguarding legitimate use of content

- *As protected systems are constantly under threat (hacking) there is a need to ensure technology is both up to date and regularly upgraded.*

How Conditional Access is attacked

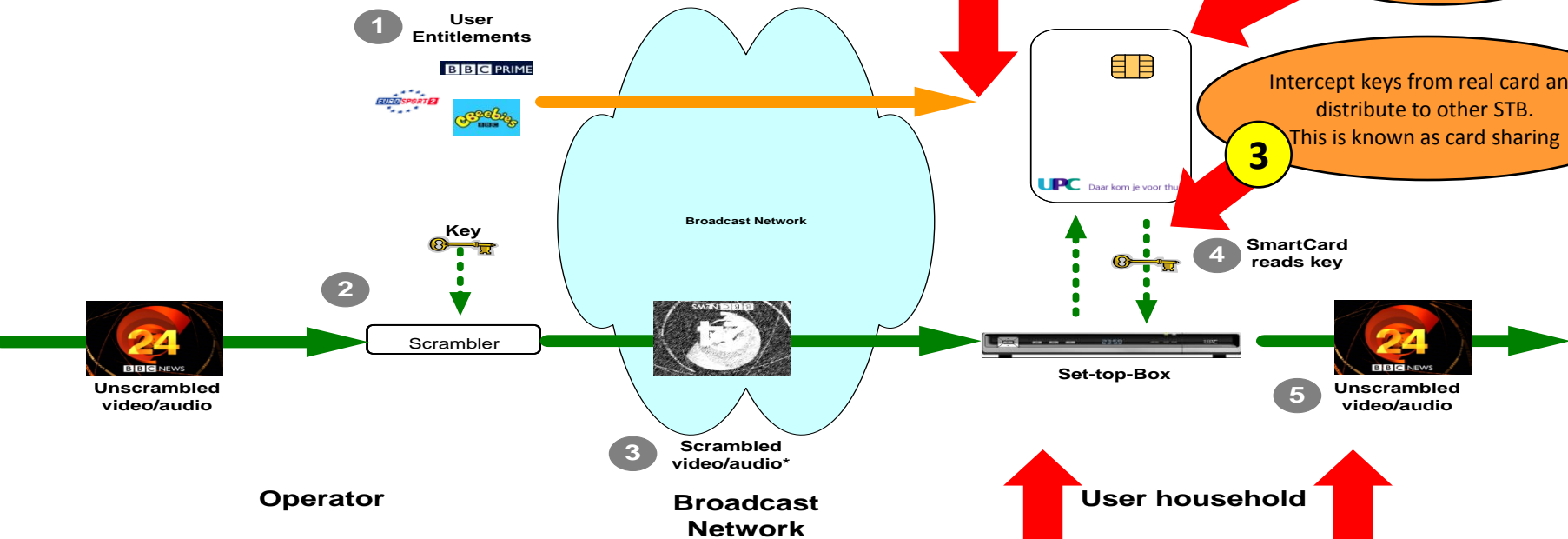
1 Modify or Block entitlement messages. Inject alternative entitlement messages. This fools a real card into allowing access

2 Create counterfeit cards that can be loaded with code to emulate a real card but with entitlements under control of a pirate

3 Intercept keys from real card and distribute to other STB. This is known as card sharing

4 Intercept and decode key – brute force attack on the scrambling algorithm itself.

5 Intercept and re-distribute analogue or digital output of STB .



1

2

3

4

5

4

5

Responses to Piracy

■ Improved Technology

□ *Legacy, Economy and Speed*

- *Protection means have to evolve with the threats and CA providers are developing more secure systems / cards and counter-measures able to resist to the pirates means.*
- *CA providers are able to modify in very short time the full behaviour of the system thus defeating non legitimate cards and receivers. This can only be achieved if it does not require any change in the standard (standard change process takes around one year).*

■ Non-technical Responses

□ *Legal prosecution*

- *Monitoring the activities of the pirates and performing legal actions against them*

- CA is the result of industry evolution from analogue pay TV for more than a decade. Today it continues to play a key role in the Audiovisual sector.
- CA is based on industry standards.
- Overall protection of Digital content requires different technologies. Conditional Access represents only one aspect of protection.
- CA protects access to broadcast and broadband services (digital/analogue, cable/air/satellite/IPTV/Mobile TV), and enables a Pay-TV business model.
- CA systems are under regular attack, as they protect highly sought-after content (movies/sports).
- CA systems need to keep evolving in order to be one step ahead of security breaches.
- Industry has been free, and must continue to be free to evolve, adapt and deploy technical solutions for content protection.