

# Card-Sharing - A new challenge for anti-piracy investigations

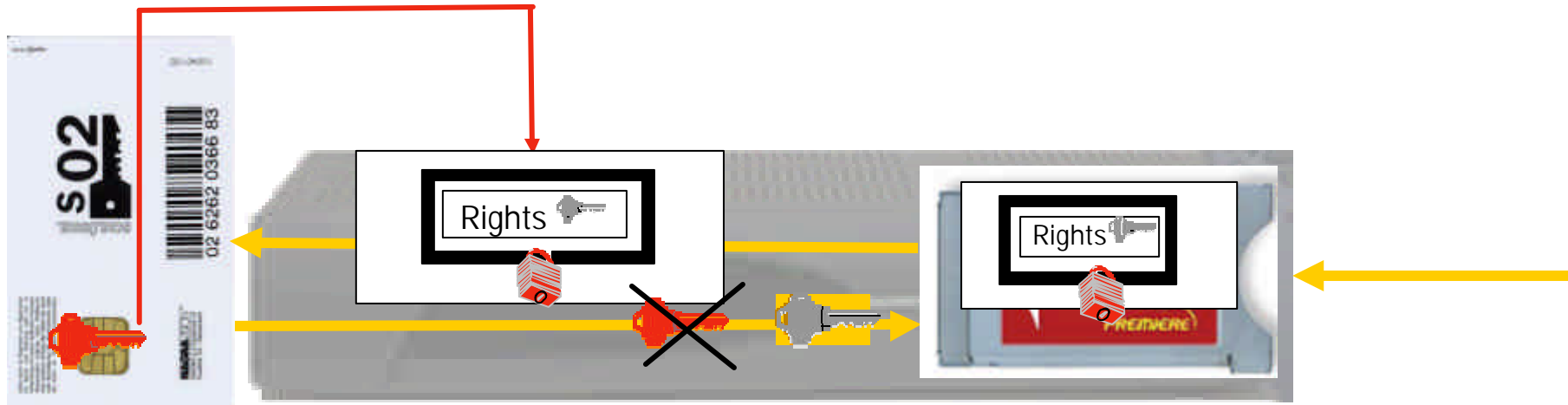
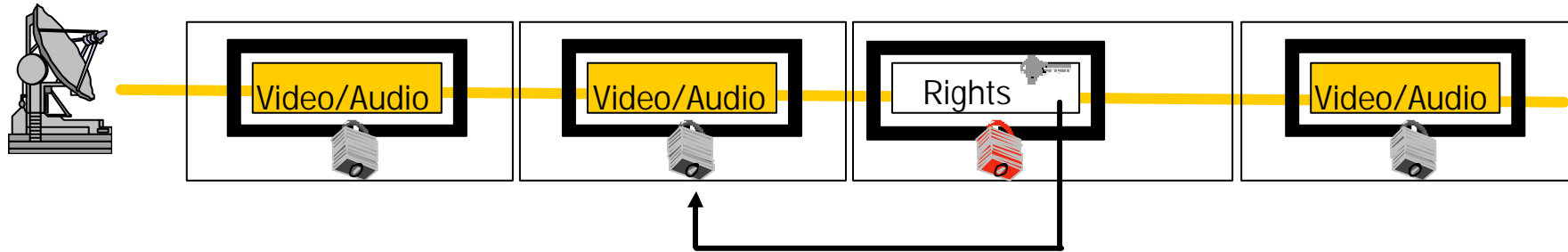
Dr. Andreas Rudloff  
Premiere Fernsehen GmbH & Co.KG

3rd AEPOC European Anti-Piracy Symposium  
London, November 22nd, 2005

- Assumptions
  - Content is dedicated only to authorized users
  - Piracy means every device or process which allows unauthorized access to protected content
  - Assumption: investigations are directed against distribution and usage of illicit devices
- Content
  - Pay TV – how it is protected
  - Pay TV – how it is attacked in the *classic style*
  - Pay TV – how it could be attacked tomorrow
  - Anti – Piracy investigations – how they are changing

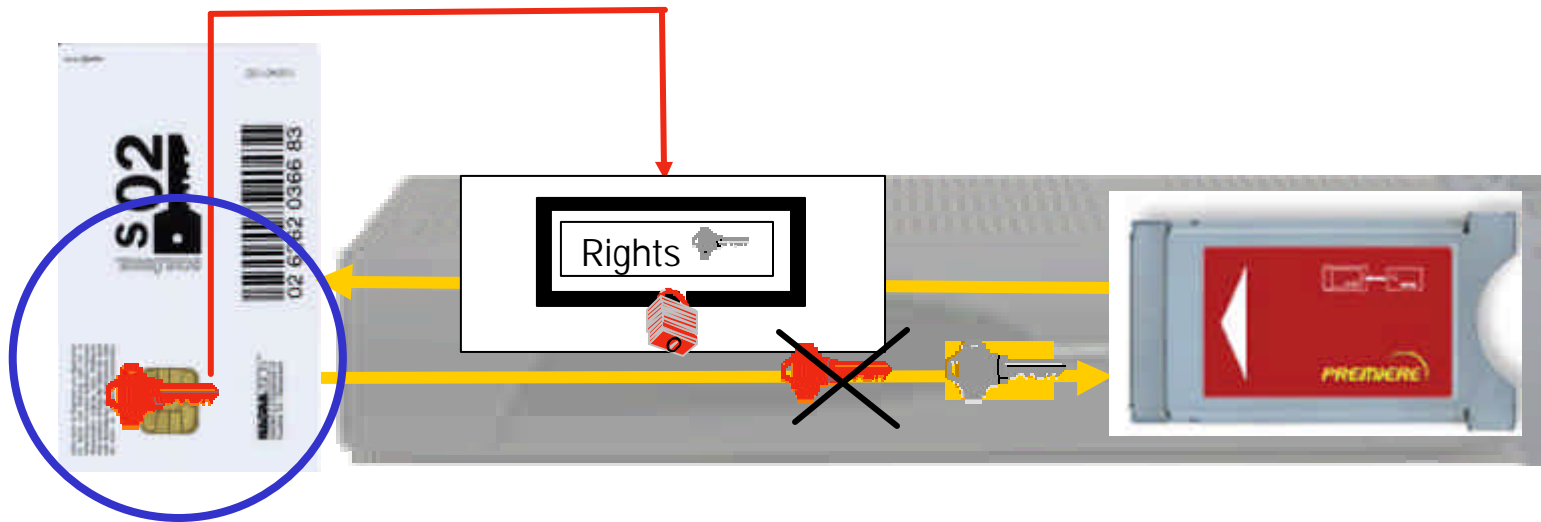
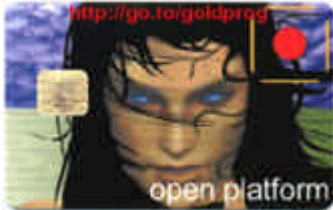
- Content protected by encryption
- Required secrets (keys/entitlements) are transmitted to authorized user and stored in the users smartcard
- System design based on the following facts
  - Content decryption can only be done in a specialised hardware, wether embedded or as external module (CI-module)
  - A secret is without any value in case it becomes obvious only after not being used any longer
  - The only device which can really be secured is a Smartcard
- Piracy means
  - Hacking the smartcard
  - Producing a physical illicit device
  - Distributing to the user is a one-time-act

# CA-Systems – general principle



# Target of piracy

- Long-living secrets (weeks and months) are the pirate ´s target
- Extracted secrets are combined with a pirate hardware to a working pirate card
- Distributed by shops and sellers

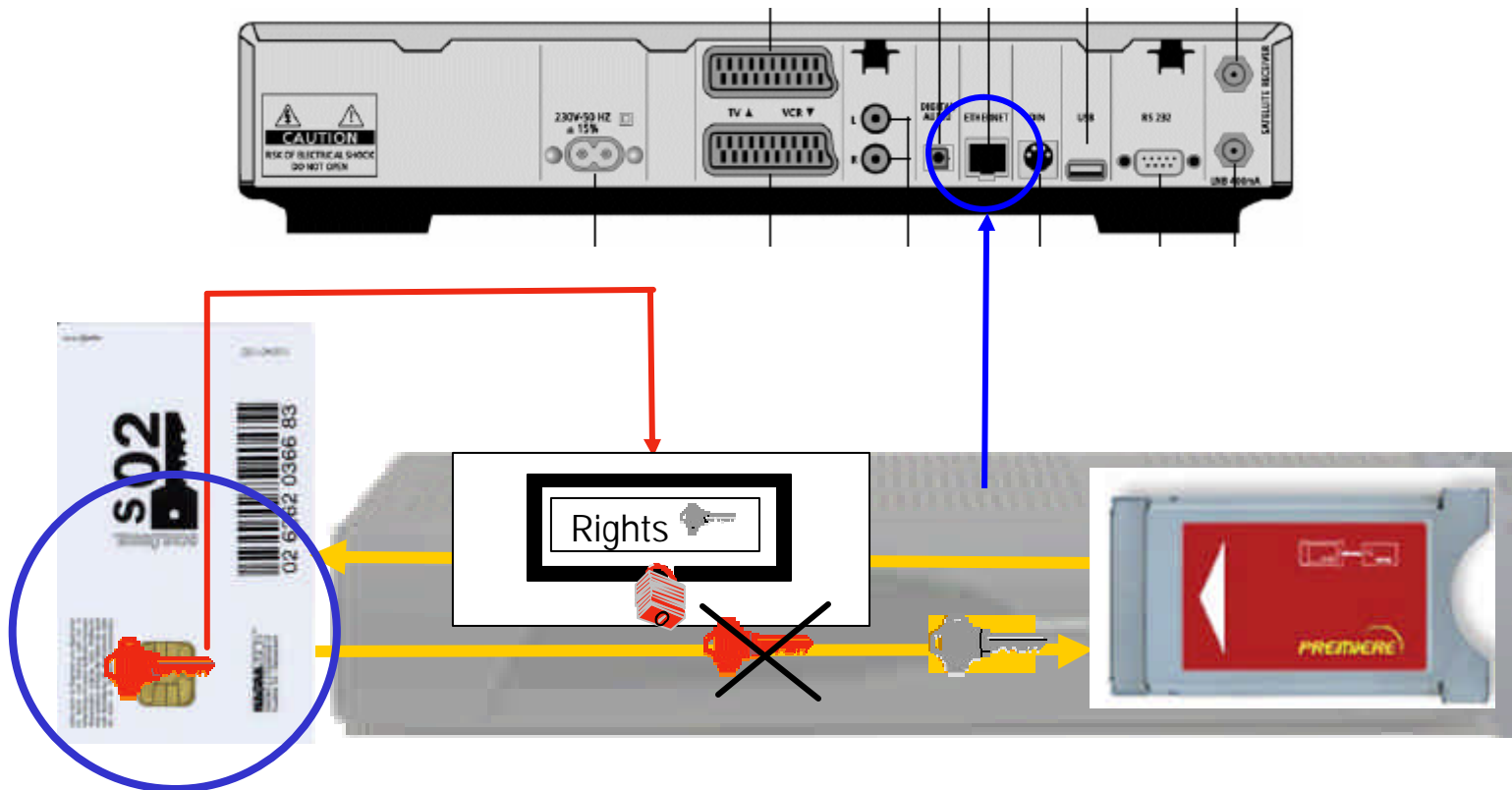


# Investigation - Classical

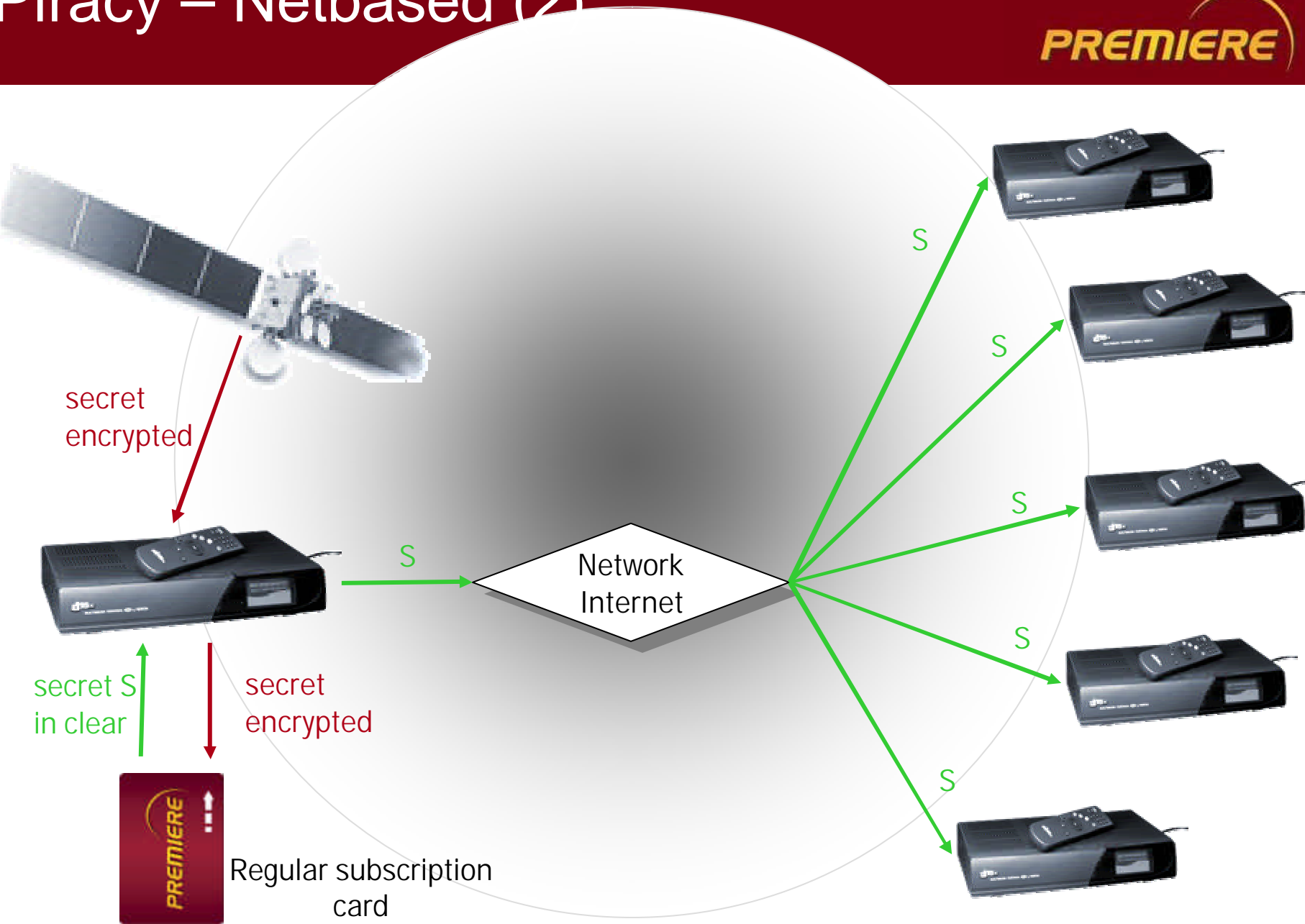
- Investigating a pirate card shop
  - Must somehow be open to public sale
  - Buying cards
- Raiding the shop
  - Ceasing technical stuff
  - Investigating the customers
- Raiding the customers
- Requirements for a good case
  - Technical evidence and forensic reports
  - An experienced investigator not necessarily an computer crime specialist
  - An fraud investigator with some IT support for forensic can do that job

# Piracy – Netbased (1)

- Changing target of piracy to short-living secrets (a few seconds)
- Real-Time distribution required

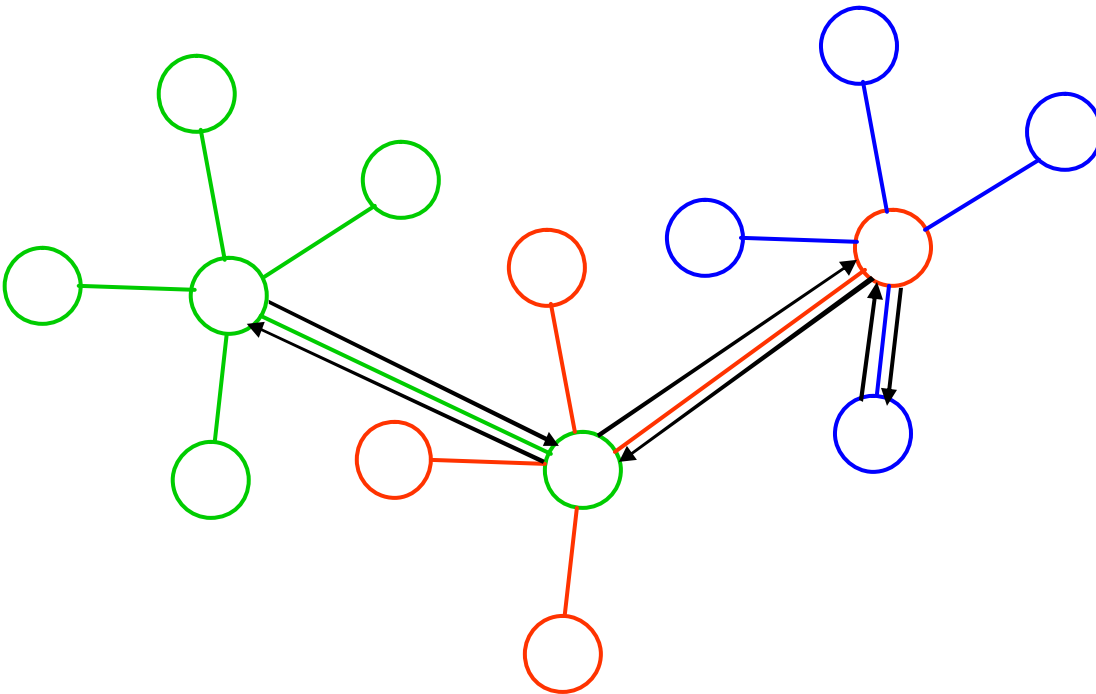


# Piracy – Netbased (2)



- Starting at the **card-sharing server**
  - determination of the IP-addresses of the customers
  - Identification of the owners of the IP-addresses
  - Raids at the customers
- Starting at the **card-sharing customer**
  - determination of the IP-address of the server
  - Identification of the owner of the IP-address
  - Raid at the server´s site
  - Identification of additional customers, see above
- Technical evidence must be collected on running systems in place
- Every thing is network connected: elimination of evidence from outside is possible
- Time pressure: technical networks are often operated by social networks
- IP-address owner´s identification: court order required, support of Internet-Providers

# Peer-to-Peer Server Structure



- Servers are only acting as proxies
- Allows pyramid selling of secrets
- Structures can be countrywide or even international
- Which law enforcement department will be in charge for such an investigation?

- Pay Content piracy begins to move to an **online piracy**
  - Online enables investigation capabilities – in theory
  - Online investigations requires education, equipment and resources for specialised teams – in practice
  - Legal framework has to support such kind of investigations
- Pay Content business moves to an **online business**
  - f.e. IPTV
  - Piracy distribution becomes easier
  - Video- and Stream-Sharing are next
- Investigation has to move to **online investigation**