KUDELSKI MAIN BRANDS AND ACTIVITY LINES

INTEGRATED DIGITAL TV
Integrated security and multiscreen user experience solutions for the monetization of digital media.

INTEGRATED DIGITAL TV
Innovative, flexible and cost-efficient solutions to deliver premium content securely over broadcast, broadband and connected devices.

INTEGRATED DIGITAL TV
Renewable Conditional Access Modules for digital TV access; full range of SD and HD set-top boxes and chipsets.

CYBER SECURITY
Tailor-made cyber security solutions and services for enterprises, financial institutions, government agencies and media customers.

PUBLIC ACCESS
Integrated access and management solutions for car parks, ski lifts, sports, entertainment and exhibition facilities.
NAGRA Digital TV: 3 Product Units

DIGITAL TV SOLUTIONS

Content & Asset Security
- anyCAST
- CAS/DRM/MDRM

Connected Devices & User Experience
- OpenTV
- STB Middleware & Applications

Multiscreen
- MediaLive
- Service Platform & Secure Player
CONNECT Clients: STB, TV, Open Devices

Set Top Box
- Hybrid broadcast/OTT
- IPTV multicast
- Pure OTT

Connected TV
- 3rd ROT or Nagra CERT

Open Devices with Secure Player
- iOS
- Android
- PC/MAC
anyCAST CONNECT

2-way embedded client for STB, Gateways and mobile devices
Includes PRM (Nagra DRM)

Supports Broadcast & OTT distribution

Security adapted for any device
Nagra HW RoT, 3rd Party RoT or pure software

Converged Security Service Platform for single product definition and SMS integration
anyCAST PRM (DRM)

- DRM for MVPD “rich” use cases
- Available on multiple devices
  - STB, iOS, Android, Mac, PC…
- Supports 1-way and 2-way use cases
  - DVR, home networking, live and on-demand OTT
- DECE and DTLA approved DRM solution for OTT and Home Networking
anyCAST CAS & PRM (DRM) in Mixed Use Cases
Merged CAS & DRM Platform - anyCAST

<table>
<thead>
<tr>
<th>Level of protection provided</th>
<th>Broadcast</th>
<th>Connected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ENABLE</td>
<td>CONNECT</td>
</tr>
<tr>
<td>Client name</td>
<td>PROTECT</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>GUARD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>COMMAND</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DRM CLIENT (OTT/Home Networking)</th>
<th>PRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Client for Basic Access to low-risk services</td>
<td></td>
</tr>
<tr>
<td>Chip-Secured Embedded Client for Medium Value Content</td>
<td></td>
</tr>
<tr>
<td>Premium Smart Card for High-Value Content</td>
<td></td>
</tr>
<tr>
<td>Next-Gen Client for Exclusive Content</td>
<td></td>
</tr>
</tbody>
</table>

MANY previous CAS and DRM platforms
Now all combined with “common crypto” including across CAS and DRM
Messaging: a CAS that works like a DRM

- Middleware manages connection Head-End
- Encrypted Media Extensions (EME) Compatible
- In Band (Broadcast) EMM no longer needed
A Single CAS/DRM Client for Hybrid Devices
Moving Security Critical Elements into the TEE

- CONNECT Client has two parts
  - CONNECT-REE & CONNECT-TEE
- Operator Pay-TV Application
  - Runs in the user space typically in Browser
  - Downloaded from App Store
  - Integrates CONNECT-REE

- Trusted Execution Environment
  - Security domain
  - With Hardware isolation from Rich OS
  - With Privileged access to platform resources
  - Provided by SOC vendors

- CONNECT-TEE is the Nagra’s Trusted Client
  - Interfaced with Nagra Root of Trust (NOCS/CERT)
FRAND - Security & Indemnification - I

- Nagra uses FRAND (actually free) content cyphers with fully disclosed operating modes
  - DVB CSA2, (CSA3), AES 128
  - Allows unilateral simulcrypt (operators can replace us somewhat economically)
  - Follows Kirchoff’s Theorem on security disclosure
  - Signaling and packet structure framework follows DVB, SCTE, HLS and MPEG-DASH standards....
FRAND - Security Indemnification - II

- Root of Trust and associated Key Ladder can be FRAND (or free i.e. ETSI) or proprietary or both
  - If we use our own proprietary one we have increased security guarantees through hidden counter measures and recovery options
  - If we use FRAND for Root of Trust and Key Ladder, the security guarantees are less as there are no hidden counter measures or recovery mechanisms
  - FRAND Root of Trust likely “keyed” by third party so indemnification further fragmented
Security as a Service

- **Who is responsible? It’s Obvious!**

- Threat models vary by network topology, network fragmentation, geographical footprint and content values

- What works today or at launch may not hold tomorrow
Device and Security Diversity

- Our customers need security on anything from a several year old smart phone to a hardened 4K capable multi-tuner home gateway / DVR
  - The same signal may have to be decrypted in a range of devices
  - Wide range of operating environments from secure processor (TEE, Secure Micro) to open SW systems
  - Wide range of security maturity in SoC suppliers
  - Wide range of features like Root of Trust in secure HW to SW emulation
  - Protected and unprotected video paths and outputs
- Permissions and security expectations vary widely and no one size fits all
  - “Best Effort” is not always a negative phrase
  - Best Effort on so many platforms requires huge efforts
Content Security, Meta Data and User Interfaces - I

- Primary content – audio, video, description, essential captioning – protected by CAS and DRM
- Additional meta data – guide descriptions, graphics, links etc. – can also be protected by CAS or DRM especially if broadcast/multicast
  - Represents a fraction of 1% in overhead
  - Represents a smaller fraction of 1% in threat model
Content Security, Meta Data and User Interfaces - II

- The extent to which a viewer or viewing device can bundle or unbundle meta-data and UEX is 99%+ a Policy decision by the operator with *little* impact on content security.
- If viewing device is breaking UEX Policy it can be revoked!
  - Requires meta-data / UEX policy and rules tied to CAS/DRM (code signing, certificates or similar) or perhaps server certificates as suggested in CVP-2...
  - Easily enforced by CAS and DRM systems or by cloud servers.
- Without a clear policy on UEX disaggregation anything and everything is possible but nothing gets focused on or accomplished?

CAS Technology and UEX Policy are 99% separable.