

DVB-H Content Encryption

Scrambling of audio-visual content for DVB-H



Features

- Real-time encryption of video (H.264/AVC) and audio (HE AACv2)
- AES-128 CTR ISMACryp compliant scrambling
- Key management with SimulCrypt environment
- Interface to Nagra key encryption (ECMG)
- Cross platform solution (Windows and Linux)

The Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut (HHI) has developed an encryption system that scrambles audio-visual content in a DVB-H environment.

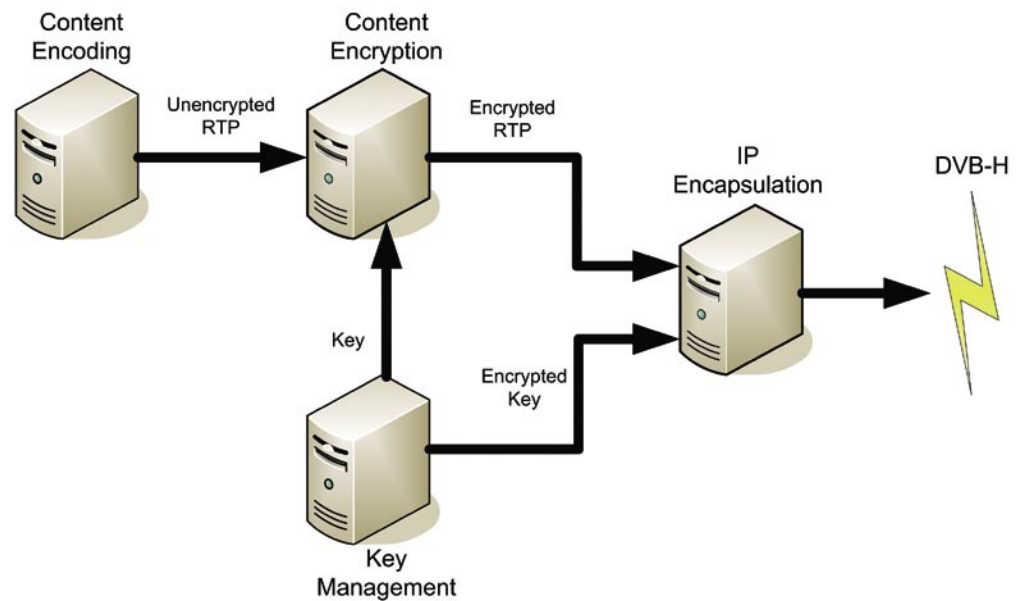
Background

DVB-H is an upcoming standard to broadcast audio-visual content to mobile handheld devices. Broadcasters world-wide see the opportunity to create and enter a new mass market by providing paid, interactive media services to a growing end-user community. For the success of the business model cryptography & key management are required to protect broadcasting channels from unauthorized access. Open standards for encryption are a groundbreaking technology that will facilitate the widespread adoption of mobile TV around the world. DVB-H solutions that are currently introduced in the market and in various field-trials all over Europe are empowered by the HHI system for content encryption and key management which is based on two open standards:

- ETSI TS 103 197 (SimulCrypt)
- ISMA TN01146 (ISMACryp)

Solution

Heinrich-Hertz-Institut provides the complete processing chain for DVB-H encoding and content scrambling.



Contact

Fraunhofer Institute
for Telecommunications
Heinrich-Hertz-Institut
Image Processing

Einsteinufer 37
10587 Berlin
Germany

Jens Güther
Phone: +49 30 31002 606
Fax: +49 30 392 72 00
Email: guether@hhi.fraunhofer.de
<http://ip.hhi.fraunhofer.de>

The diagram shows the complete DVB-H encoding and scrambling system that comprises the following processing steps:

- Grabbing of the A/V input signal (analog or digital SDI)
- A/V compression based on MPEG-4 AAC and H.264/AVC
- RTP streaming according to RFC3640/RFC3984
- Content scrambling utilizing SimulCrypt and ISAMCryp standards
- Streaming of encrypted RTP packets (RFC3640)
- Communication with the IP encapsulation device.

The software is highly modular and is available for Linux as well as for Windows systems.