



Fraunhofer

IIS

FRAUNHOFER INSTITUTE FOR INTEGRATED CIRCUITS IIS

HECA HIGH EFFICIENCY CONDITIONAL ACCESS FOR DIGITAL BROADCASTING SERVICES



WHAT IF ALL DIGITAL RADIO USERS WOULD PAY FOR YOUR PREMIUM INFORMATION SERVICES?

These days, people are willing to pay money to make their hectic lives that little bit easier. Finding the closest parking spot, receiving the latest news via car radio or watching a favorite soap opera over mobile TV: digital broadcasting is the cheapest and most convenient way to deliver these and other data services to a large mobile audience. Regardless of what service you are planning, HECA is the key to monetize such services.

HECA solutions by Fraunhofer IIS enable controlled distribution and consumption of digital content through efficient conditional access technology, specifically tailored for digital broadcasting.



HECA MARKETS

Service Provider

Protecting a data service from unauthorized access is crucial for the success of any business model entailing the broadcasting of premium information. At the same time, there is a desire to make the most of the available data rate and convey as much information as possible. Unlike some conventional Conditional Access systems, HECA requires only a small data overhead for management messages. This leaves most of the available bandwidth for information services. Furthermore, receiving devices do not need a back-channel to confirm reception of messages as they are transmitted permanently.

HECA allows for the flexible generation of service bundles and helps service providers to realize new business models. A service may contain scrambled and unscrambled parts at the same time. For example, headlines could be readable by all users of a news service (free-to-air), while only subscribers of the service have full access to the complete story. HECA supports different types of service models, including service subscription for a certain period of time, allocation of lifelong rights, and pay-per-use applications.

FRAUNHOFER OFFERS HECA SERVER SYSTEMS TO PROTECT INFORMATION SERVICES EASILY AND EFFECTIVELY.

Receiver manufacturers

HECA is included in the TPEG Automotive Profile and is implemented in DAB/MOT, DRM/MOT and DRM/Sub-channel. To be able to make forthcoming information services available to consumers, manufacturers will need to integrate HECA decoders in the next generation of receivers. Depending on the hardware design of the end-user device and security needs of the service provider, HECA decoders can be implemented in a pure software setting or in a highly secure crypto hardware environment. HECA's cryptographic core is based on the AES algorithm, which is intended for integration into devices with limited computational complexity and performance. HECA has already been integrated into BMW and Audi prototype equipment.

HECA IS AN OPEN STANDARD AND FRAUNHOFER OFFERS CUSTOMIZED DECODER SOFTWARE IMPLEMENTATIONS.



HECA TECHNOLOGY

Security

HECA employs a multi-level key hierarchy. The applied cryptographic algorithms for scrambling, descrambling and message authentication are based on the AES algorithm. Different key lengths and cipher-modes are used.

HECA also enables the parallel operation of receivers with different security levels – for example, Personal Navigation Assistants (PNAs) or OEM navigation devices in cars. Obtaining a key for a specific terminal family does not compromise the security of other device families.

HECA PRODUCTS

FRAUNHOFER OFFERS THE FOLLOWING PRODUCTS:

- HECA DECODER MODULE
- HECA INITIALIZATION SERVER
- HECA ENTITLEMENT SERVER
- HECA ENCRYPTION SERVER

HECA Decoder Module

HECA Decoder module decodes, verifies and processes the management messages, evaluates security keys and descrambles the service data.

It is designed for PCs or OEM devices, and suitable for easy integration in low-cost mobile devices without back-channel, for example Personal Navigation Assistants (PNAs) and mobile phones.

Fraunhofer IIS offers the HECA Decoder module for embedded environments with optional adaptations for specific target platforms and security concepts. Porting HECA onto Smart Cards is also possible. The HECA Decoder specification can be obtained through TISA (Traveller Information Services Association, www.tisa.org).

HECA Initialization Server

The HECA Initialization Server generates and delivers unique device-IDs and high secure device keys based on the requirements of the device producer.

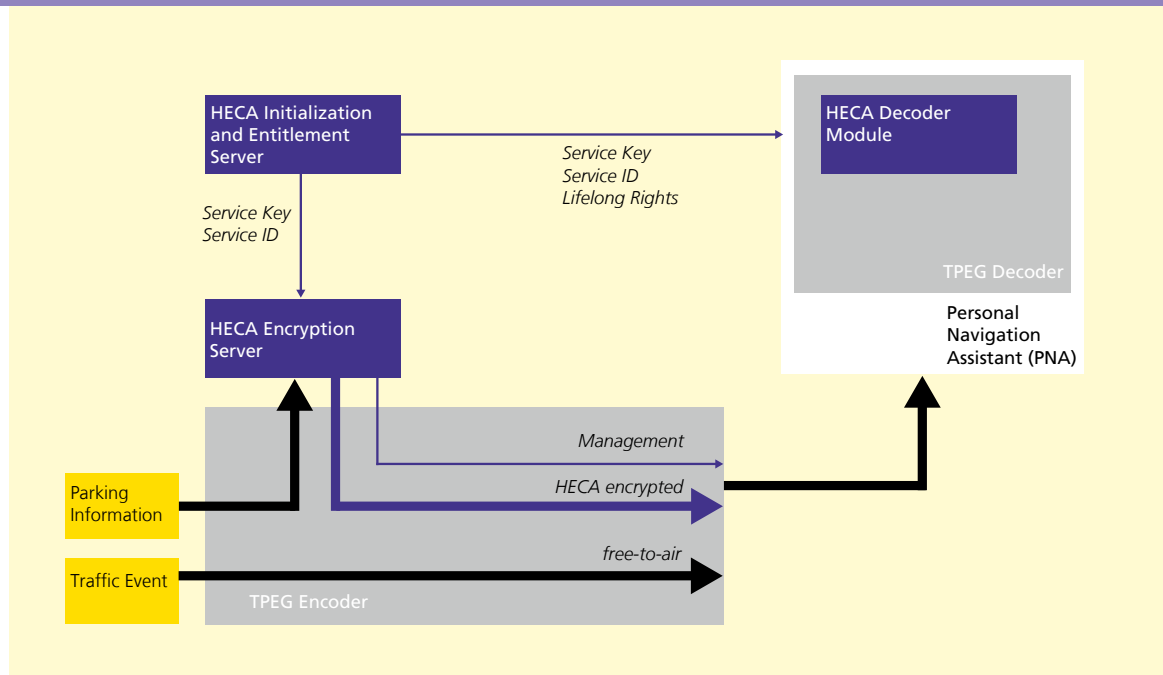
HECA Entitlement Server

At the request of a service provider, the HECA Entitlement Server configures services and stores the entitlements and subscriptions together with corresponding service keys in an internal or external database. It controls the service set-up and service duration as well as token reload, and generates corresponding EMMs (Entitlement Management Messages).

HECA Encryption Server

The HECA Encryption Server scrambles service data with the corresponding control word, periodically generates ECMs (Entitlement Control Messages), and feeds both into the transmission chain.

How HECA works with TPEG, the traffic information system. A TPEG service contains free-to-air components (traffic event) and premium components (parking information). HECA protects the premium information from unauthorized access.



HECA SOLUTIONS BY FRAUNHOFER ARE NOW AVAILABLE AS INDIVIDUAL COMPONENTS OR IN COMBINATION WITH OTHER FRAUNHOFER PRODUCTS SUCH AS AUDIO AND VIDEO CODECS, DIGITAL BROADCASTING ENCODERS OR IP STREAMING SOLUTIONS.

For more information about HECA, please visit

WWW.IIS.FRAUNHOFER.DE/AMM

**Fraunhofer Institute for
Integrated Circuits IIS**

Executive Director
Prof. Dr.-Ing. Heinz Gerhäuser
Director
Prof. Dr.-Ing. Günter Elst

Am Wolfsmantel 33
91058 Erlangen
Phone +49 9131 776-0
Fax +49 9131 776-999
info@iis.fraunhofer.de
www.iis.fraunhofer.de

Contact
Birgit Bartel-Kurz
Phone +49 9131 776-6175
amm-info@iis.fraunhofer.de

**Fraunhofer USA, Inc.
Digital Media Technologies***

100 Century Court
Suite 504
San Jose, California 95112
www.dmt.fraunhofer.org

Contact
Phone +1 408 573 9900
codecs@dmf.fraunhofer.org

* Fraunhofer USA Digital Media Technologies, a division of Fraunhofer USA, Inc., promotes and supports the products of Fraunhofer IIS in the U. S.

About Fraunhofer IIS

The Fraunhofer IIS Audio and Multimedia division, based in Erlangen, Germany, has been working in compressed audio technology for more than 20 years and remains a leading innovator of technologies for cutting-edge multimedia systems. Fraunhofer IIS is universally credited with the development of mp3 and co-development of AAC (Advanced Audio Coding) as well as technologies for the media world of tomorrow, including MPEG Surround, MPEG Spatial Audio Object Coding and the Fraunhofer Audio Communication Engine.

Through the course of more than two decades, Fraunhofer IIS has licensed its audio codec software and application-specific customizations to at least 1,000 companies. Fraunhofer estimates that it has enabled more than 1 billion commercial products worldwide using its mp3, AAC and other media technologies.

The Fraunhofer IIS organization is part of Fraunhofer-Gesellschaft, based in Munich, Germany. Fraunhofer-Gesellschaft is Europe's largest applied research organization and is partly funded by the German government. With nearly 15,000 employees worldwide, Fraunhofer-Gesellschaft is composed of 57 Institutes conducting research in a broad range of research areas.