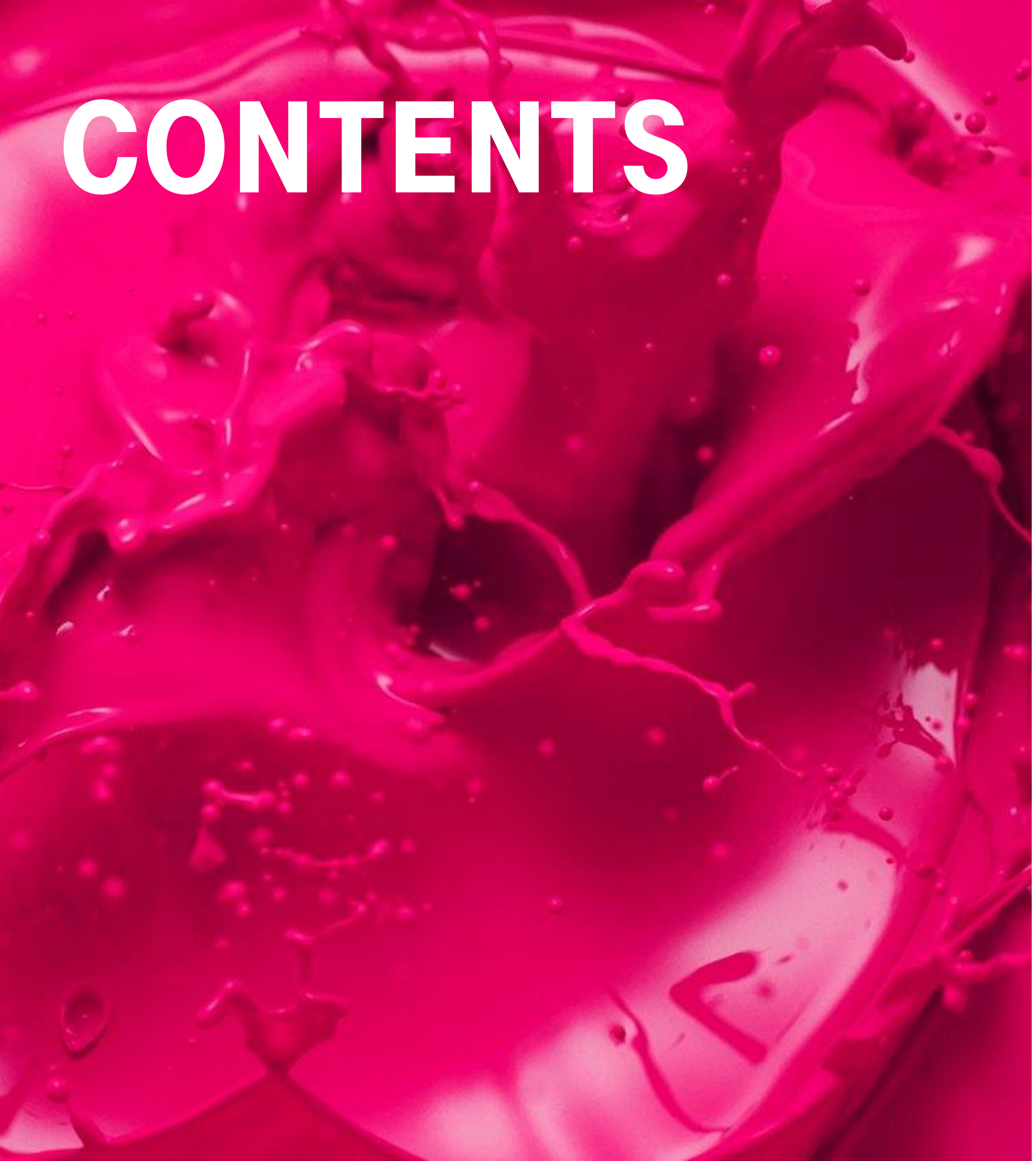
ADVANCED ECOSYSTEM FOR CONTENT PROTECTION

Dr. Jens Johann, Deutsche Telekom

LIFE IS FOR SHARING.

CONTENTS



ITUEvents

ITU workshop on the future of television for Europe

7 June 2019
ITU headquarters
Geneva, Switzerland

http://itu.int/go/TV-Europe

Follow us on twitter @ITU_EUR

Workshop organized within the framework of the ITU Regional Initiatives for Europe and the ITU Study Groups responsible for standardization of Television, namely ITU-T SG9 and ITU-R SG6

- Introduction
- Embedded Common Interface ECI
- ECI - Architecture and Components
- Trust Environment
- Standardization Activities
- Summary

INTRODUCTION

DTAG ACTIVITIES IN MEDIA DISTRIBUTION

Deutsche Telekom offers MagentaTV for their customers and is starting now with OTT offers

- Up to 100 channels from public and private broadcasters
- Supported content formats: SD, HD, UHD, HDR
- Access to premium content
- Access to TV media libraries of several providers
- Additional booking of special interest channels
- Service control possible via „TV app“ in home and mobile networks

Number of customers in Germany (EOY 2018): 3.3 Mio.

More and more offers need a flexible and easy-to-manage content protection scheme to fulfil requirements of content owners and the wish of consumers not to be bothered by technical details

SOME THOUGHTS ON CONTENT PROTECTION

Content aggregators and service providers would like to

- reach as many devices as possible in a safe way
- decrease costs for play-out extensions
- minimize downtime for updates and the implementation of extensions
- support different content protection schemes in the consumer device

Business needs

- Increase of Interoperability
- Support open eco system for market development
- Encourage CA/DRM vendors to develop competitive solutions
- Avoid “Lock-in” situations for platform operators and customers
- Avoid necessity for hardware modules (reduced costs)

A VIEW ON THE MARKET

Protected content distributed over classical broadcast and broadband networks to an increasing number of CPEs (iDTV, STB, tablets, sticks and consoles,...)

Many solutions in the market for delivery of linear TV and VoD services in HD and UHD resolution via managed and unmanaged networks with dependencies for platform operators and consumers

Proprietary solutions as well as parallel existing protocols and technologies with impact on interoperability of CPE concerning service offerings, e.g. related to:

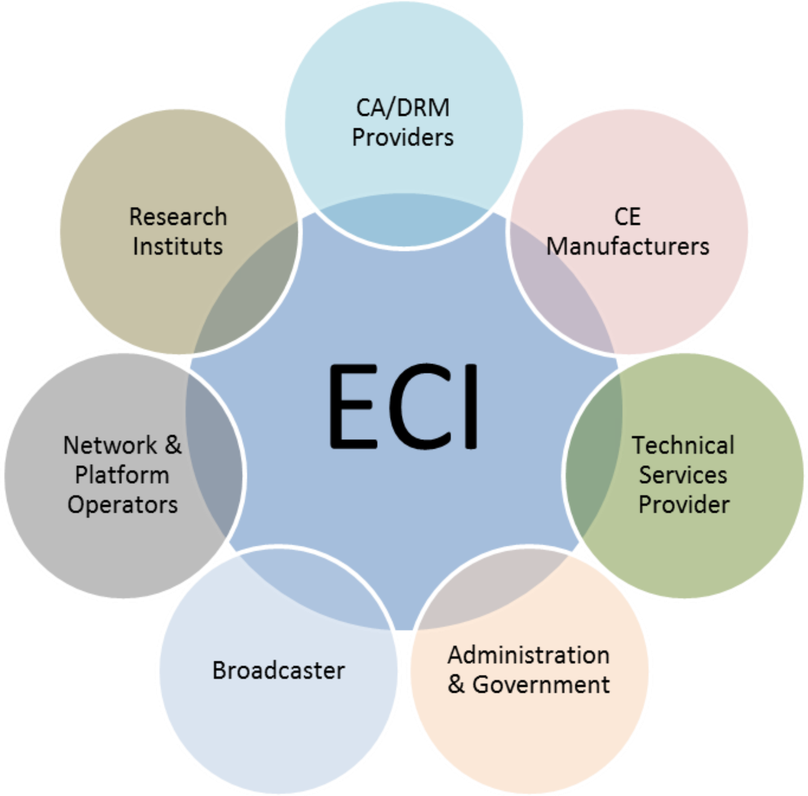
- Conditional Access / Digital Rights Management (CA/DRM)-Systems
- Middleware
- Signalling protocols
- Audio and video codecs
- Further platform specific features

➔ Fragmented market

LIFE IS FOR SHARING.

EMBEDDED COMMON INTERFACE ECI

ECI BACKGROUND & ESSENTIALS

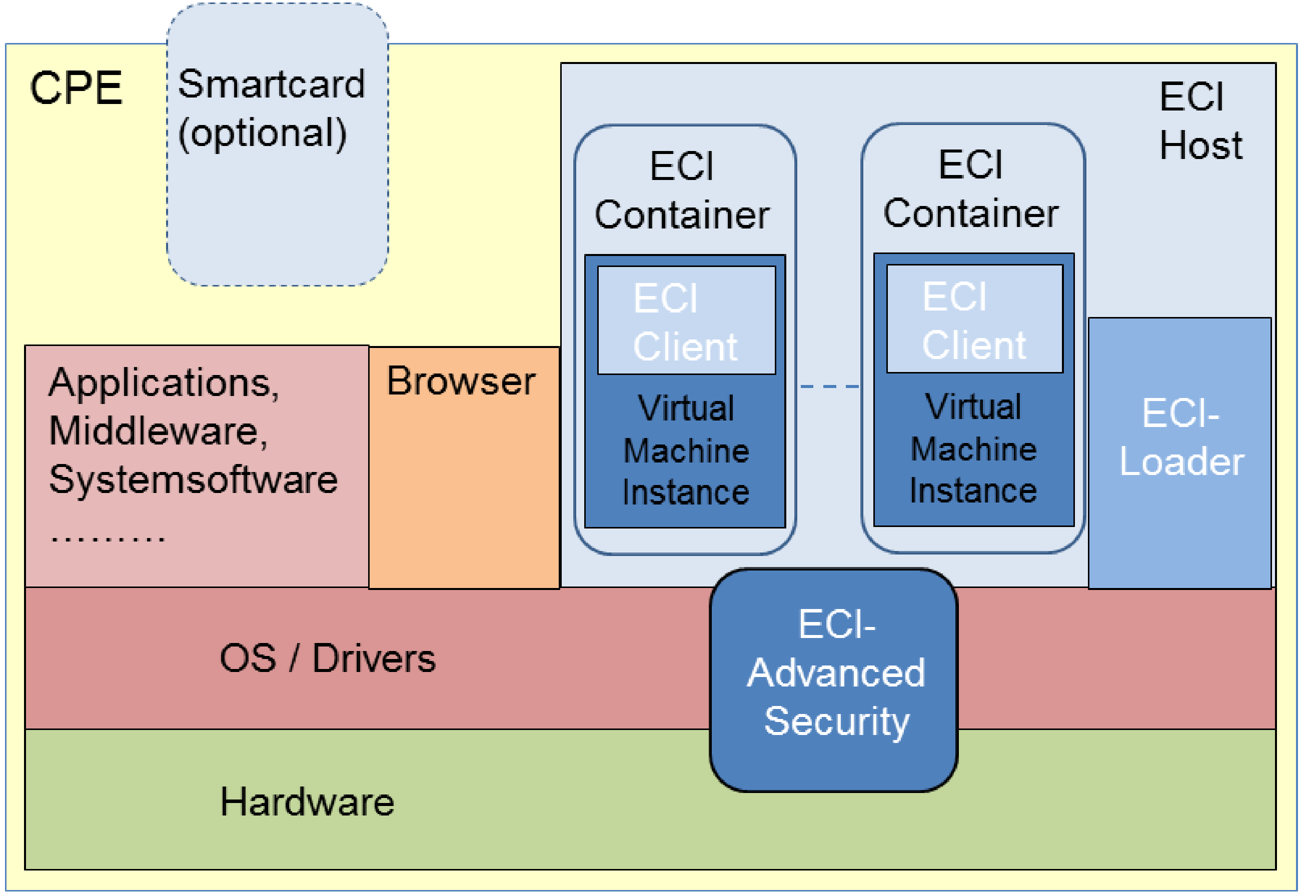

CA/DRM Providers
CE Manufacturers
Technical Services Provider
Administration & Government
Broadcaster
Network & Platform Operators
Research Instituts
ECI

ECI: Embedded Common Interface for exchangeable CA/DRM solutions

- Initiative by representatives of the value chain to develop a standardized solution for content protection
- Work organized in ETSI between 2014 and 2018 in close collaboration with ITU-T SG9 (Q2/9), with focus on:
- Standardized APIs for the exchange of CA/DRM systems (ECI Clients) (ECI does not standardize the CA/DRM system itself)
- Exchangeable, embedded ECI Clients by SW download in broadcast and broadband environments
- Multi-ECI-Client architecture
- Standardized enhanced security-related mechanisms
- Exchange of ECI Clients embedded in a Trust Environment

ECI - ARCHITECTURE AND COMPONENTS

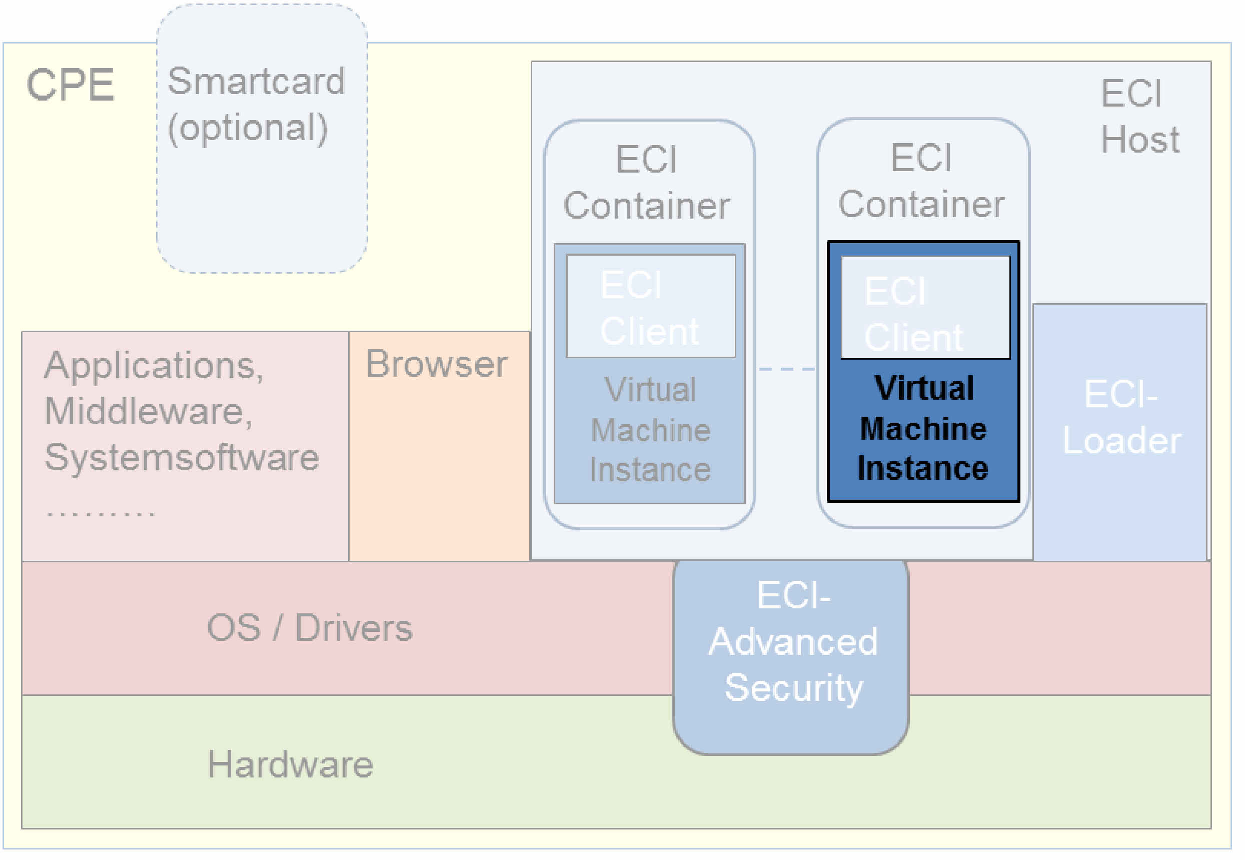
ARCHITECTURE



- ECI does not specify special CPE features nor CA/DRM functionalities. The core elements of the ECI specifications are the APIs between the ECI Client and the ECI Host.
- The implementation of the ECI Host is under responsibility of the CPE manufacturer, in line with the ECI specifications and the compliance & robustness regime.
- The implementation of the ECI Client is under responsibility of the CA or DRM vendor, in line with the ECI specifications and the compliance & robustness regime.
- Each API has its version management, allowing for profiling and future extensions.

THE VIRTUAL MACHINE (VM)

- The Virtual Machine is the software environment, in which the ECI Client is executed.
- The VM interfaces to the ECI Host are providing access to the necessary resources of the CPE.
- Each ECI Client has its own VM Instance.

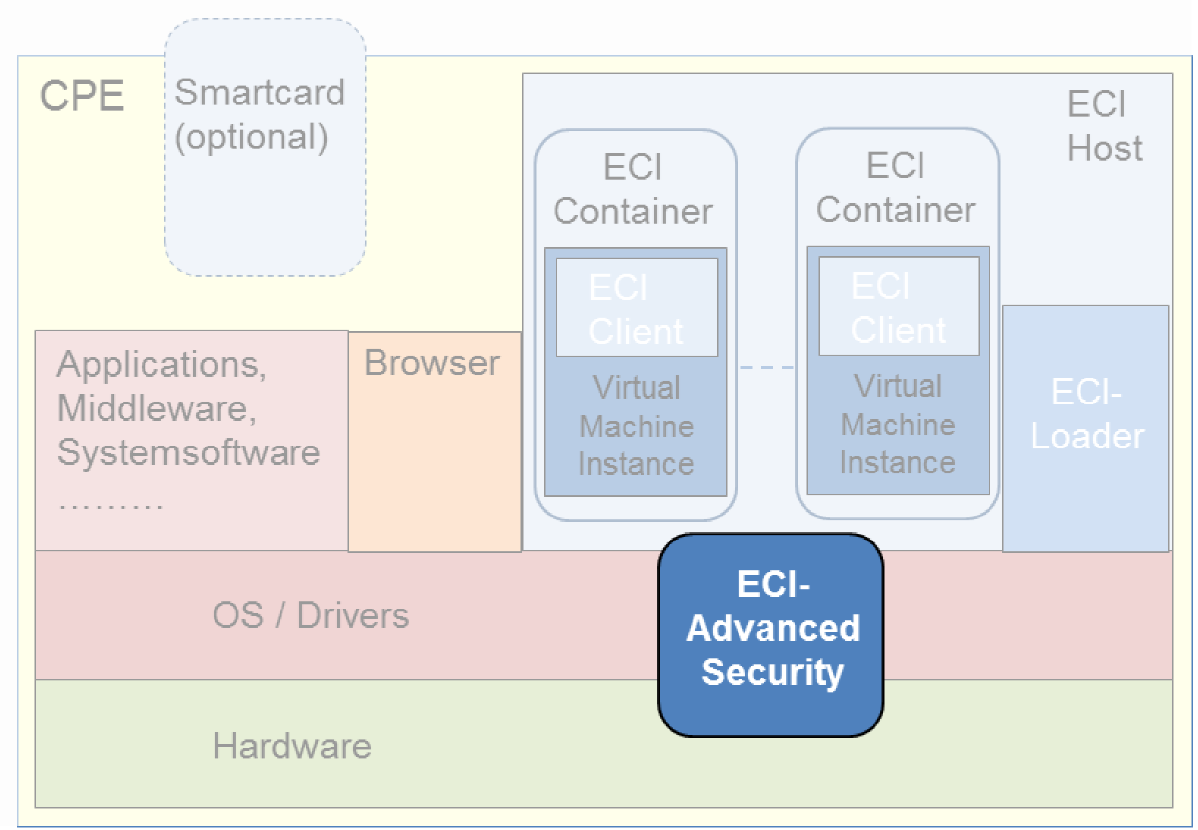


ADVANCED SECURITY (AS)

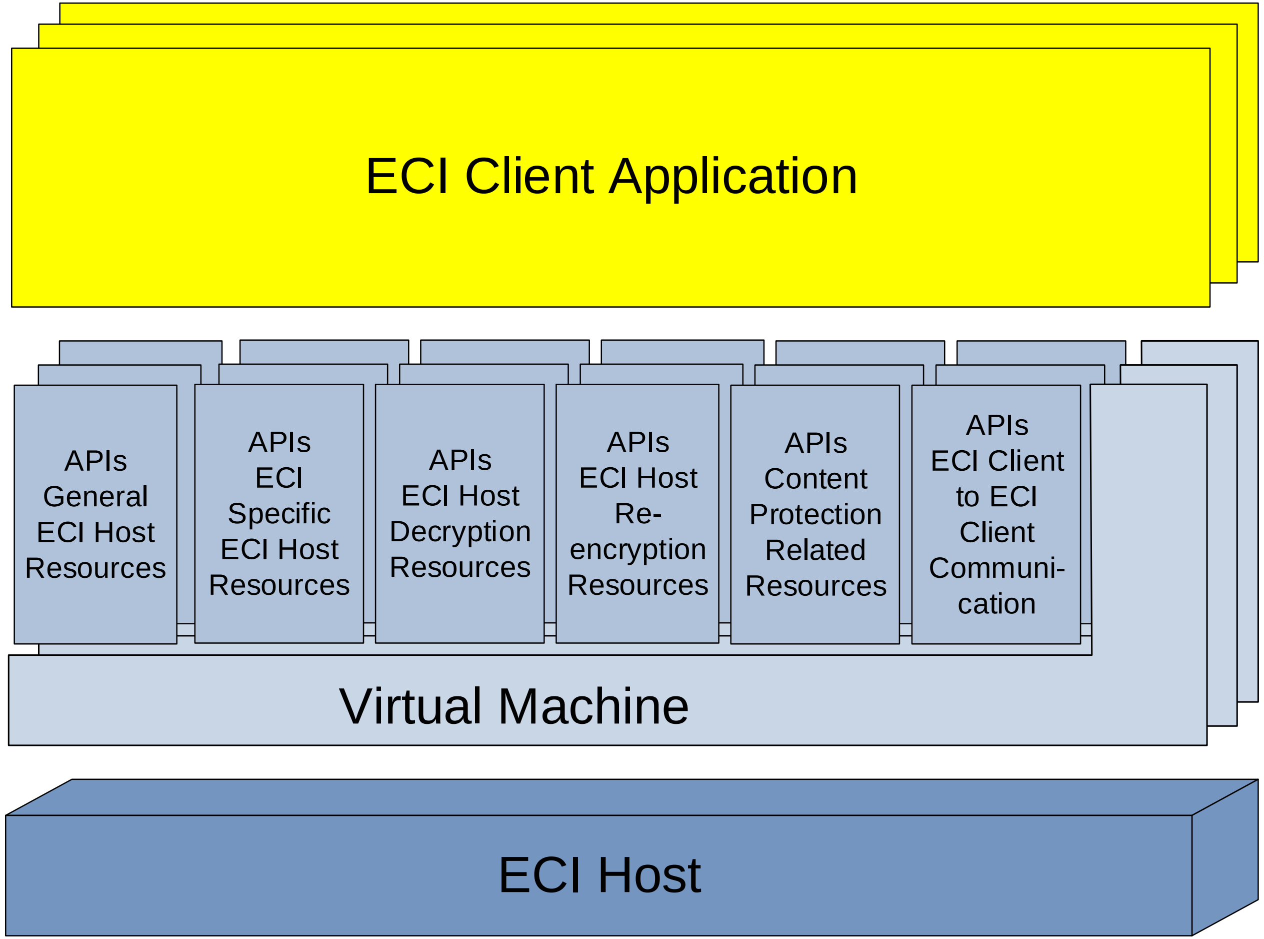
Advanced Security adds hardware security functions to the ECI System:

- Enhanced Key Ladder
- Certificate processing system
- Renewability functions
- Compatible with current CPE chip architectures

Advanced Security provides tools to an ECI Client, allowing to enhance the security of different relevant processes.



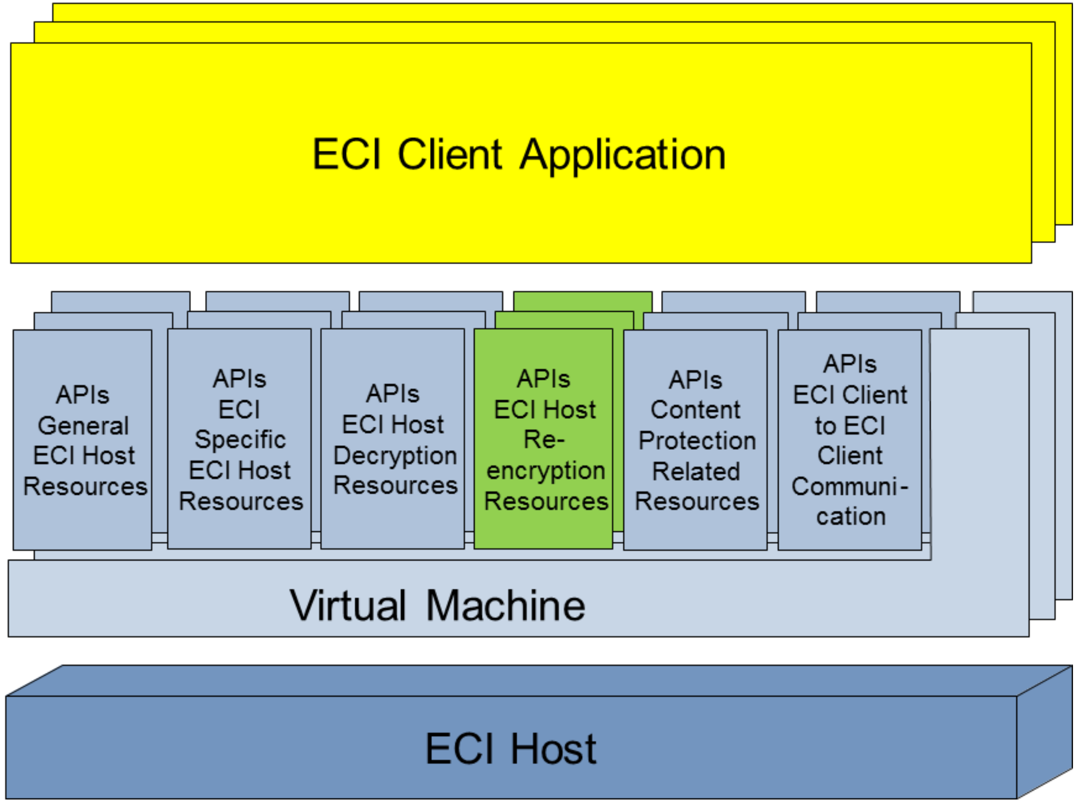
THE APIS OF THE ECI SYSTEM


ECI Client Application
APIs General ECI Host Resources
APIs ECI Specific ECI Host Resources
APIs ECI Host Decryption Resources
APIs ECI Host Re-encryption Resources
APIs Content Protection Related Resources
APIs ECI Client to ECI Client Communi-cation
Virtual Machine
ECI Host

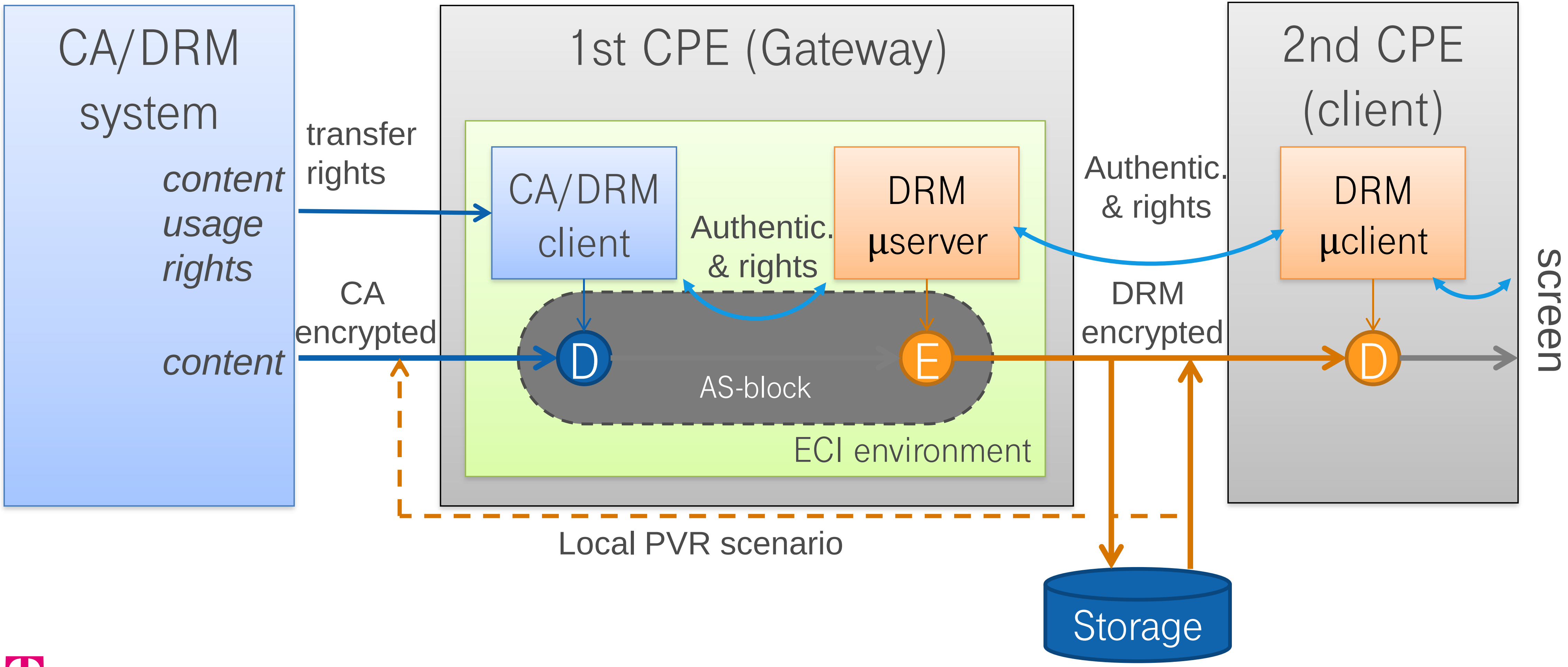
- APIs give an ECI Client access to all relevant resources of a compliant CPE

EXAMPLE: RE-ENCRYPTION OF CONTENT

- Client to inform Host about decryption support
- Special Client called Micro Server to offer its re-encryption capabilities to the Host
- Content can be decrypted and re-encrypted for storage or export to other devices
- Content decryption and re-encryption done by Host, authentication and rights provided by Client and Micro Server


ECI Client Application
APIs General ECI Host Resources
APIs ECI Specific ECI Host Resources
APIs ECI Host Decryption Resources
APIs ECI Host Re-encryption Resources
APIs Content Protection Related Resources
APIs ECI Client to ECI Client Communi-cation
Virtual Machine
ECI Host

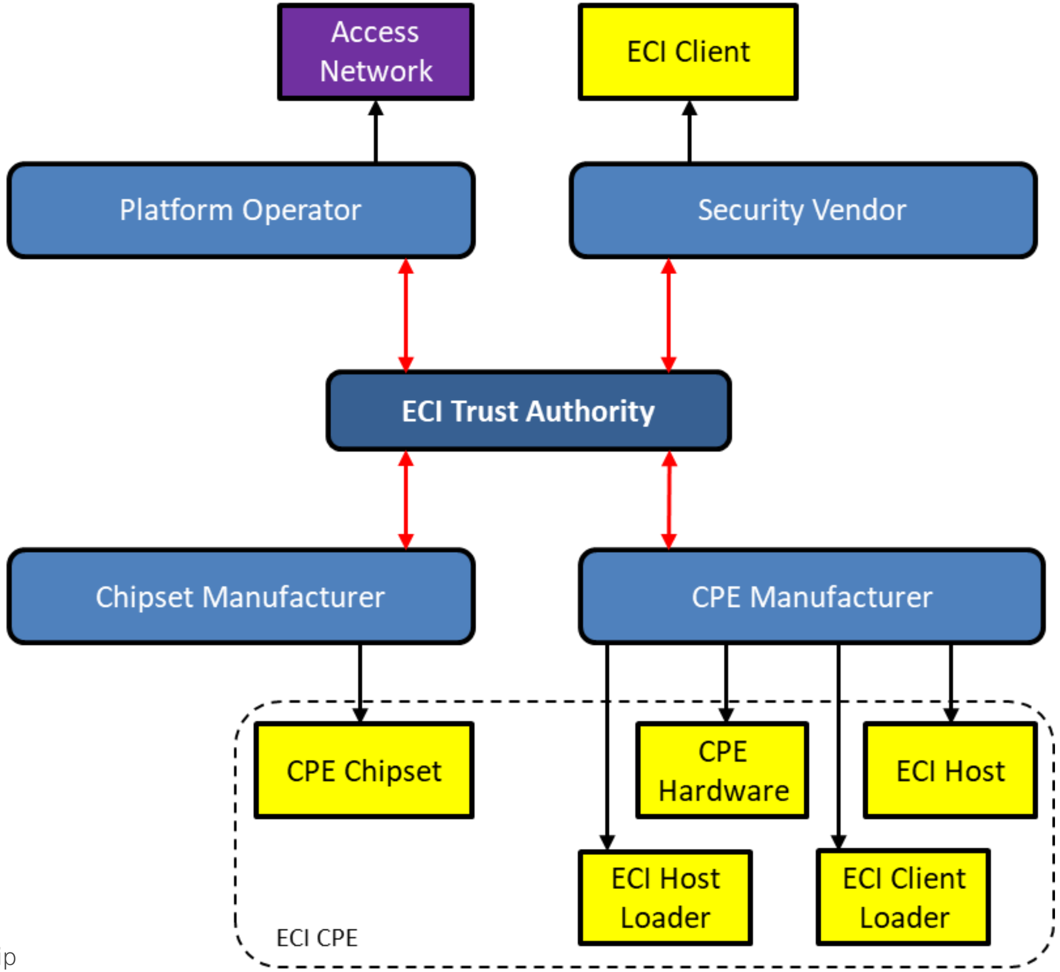
EXAMPLE: RE-ENCRYPTION OF CONTENT



TRUST ENVIRONMENT

TRUST ENVIRONMENT: KEY STAKEHOLDERS

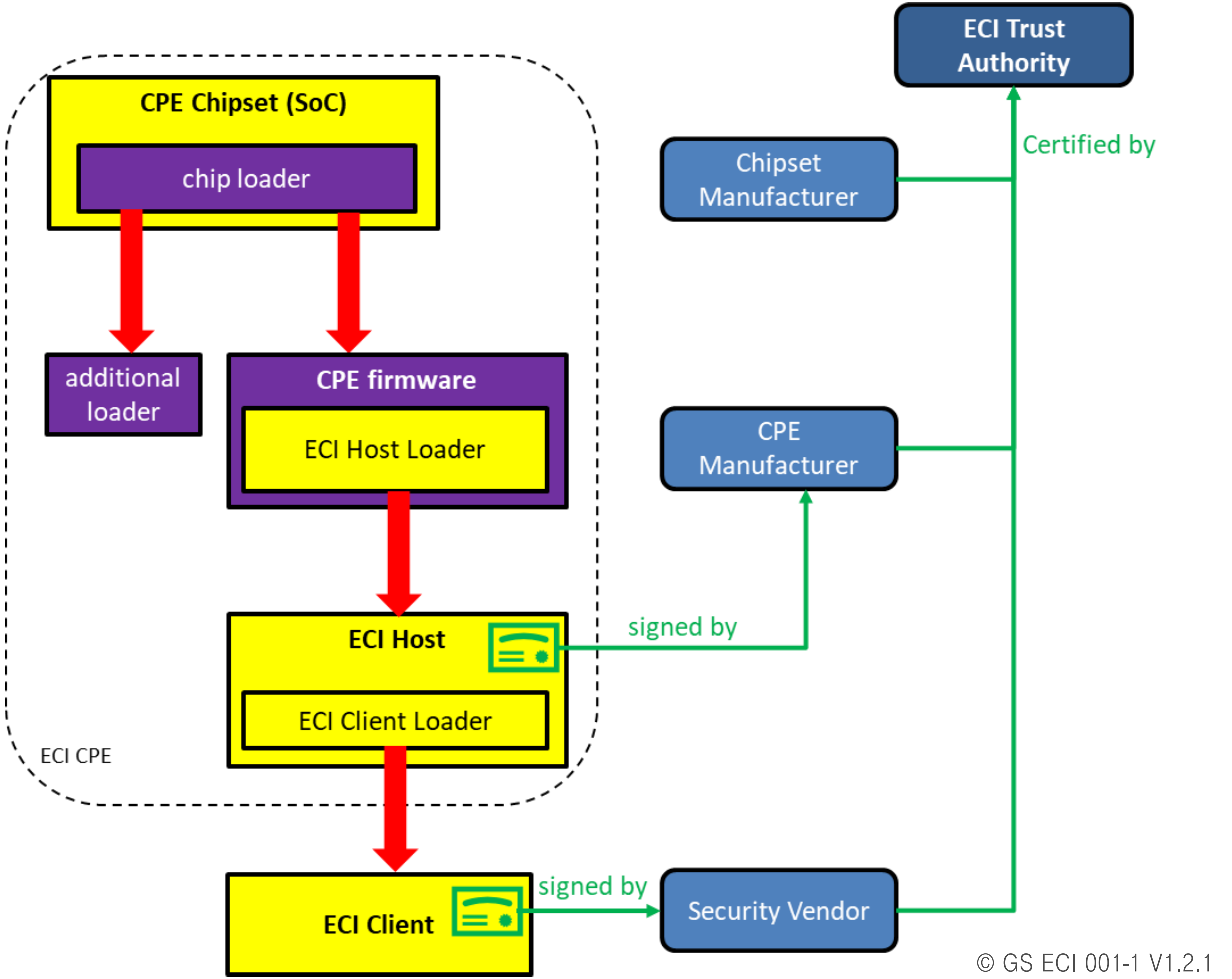
- The ECI Trust Authority is the driving force in an ECI eco system
- The four key stakeholders form the basis of an ECI eco system.
- The stakeholders may, and most likely will, interact with each other.



* Red arrows indicate a contractual relationship
* Black arrows indicate entities or services created by a stakeholder

TRUST ENVIRONMENT: CERTIFICATE HIERARCHY

- ECI Entities are signed by their creators.
- The creators have their keys signed by the Trust Authority.
- This creates a chain of trust from the Trust Authority to the signed Entity.
- Revocation of an Entity is done by the creator that signed it.



© GS ECI 001-1 V1.2.1

STANDARDIZATION ACTIVITIES

ITU-T ACTIVITIES RELATED TO ECI

ITU-T Recommendations specifying the ECI Ecosystem (J series)

Published ITU-T Recommendations (09/2016):

- **J.1010**: "Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements"
- **J.1011**: "Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview"

Determined ITU-T – Recommendations (TAP, Res 1):

- **J.1012** (ex J.dmcd-part3): "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; CA/DRM Container, Loader, Interfaces, Revocation"
- **J.1013** (ex J.dmcd-vm): "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; The Virtual Machine"
- **J.1014** (ex J.dmcd-eci-as): "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Advanced Security – ECI-specific functionalities"
- **J.1015** (ex J.dmcd-kl-as): "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; The Advanced Security system – Key Ladder Block"
- **J.1015.1** (ex J.dmcd-kl-as Annex A): "Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; The Advanced Security system – Key Ladder Block: Authentication of control word usage rules information and associated data 1"

ITU-T ACTIVITIES RELATED TO ECI

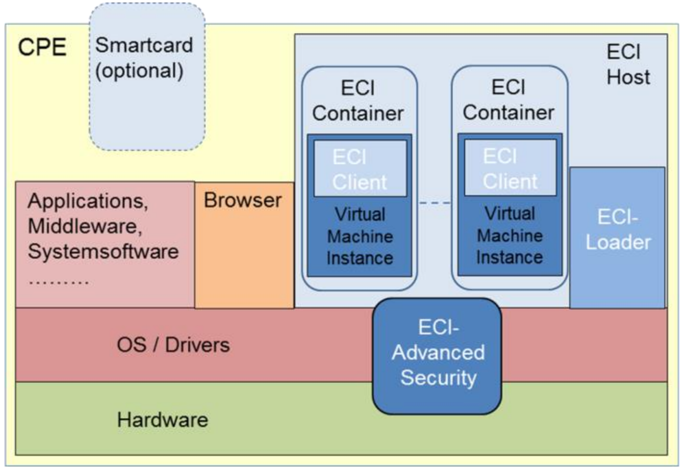
ITU-T Supplements Complementing the ECI Ecosystem (Final Drafts for Approval)

- **J Suppl.7** (ex. J.sup-eg): “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; ECI Guide (EG)”, including recommended ECI performance values, use cases and scenarios associated with an ECI Ecosystem
- **J Suppl.8** (ex. J.sup-te): “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Trust Environment (TE)”, covering stakeholders, roles and tasks of an ECI Trust Authority and addressing critical workflows within the ECI Ecosystem
- **J Suppl.9** (ex. J.sup-val): “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; System Validation (VAL)”, covering test cases and flow diagrams for ECI Host and Client installation procedures, decryption, re-encryption and play-out to external devices

SUMMARY

ADVANTAGES OF THE ECI ECOSYSTEM

- ECI does not require any hardware replacement in case the CA- or DRM-Client has to be replaced in a CPE: just download a new software Client
- ECI offers standardized Advanced Security hardware support which allows the implementation of state of the art CA/DRM solutions
- ECI can be easily implemented in today’s CPE chipsets, based on the open security architectures of chip vendors
- ECI is easily applicable in broadcast and broadband environments
- ECI leverages cost savings for all relevant stakeholders of the Digital Media Business
- ECI offers the consumer the requested flexibility for choice of services from different content providers and platform operators



CONTACT

DR. JENS JOHANN
J.JOHANN@TELEKOM.DE