Conditional Access with Java Card^{TM} and DReaM-CAS

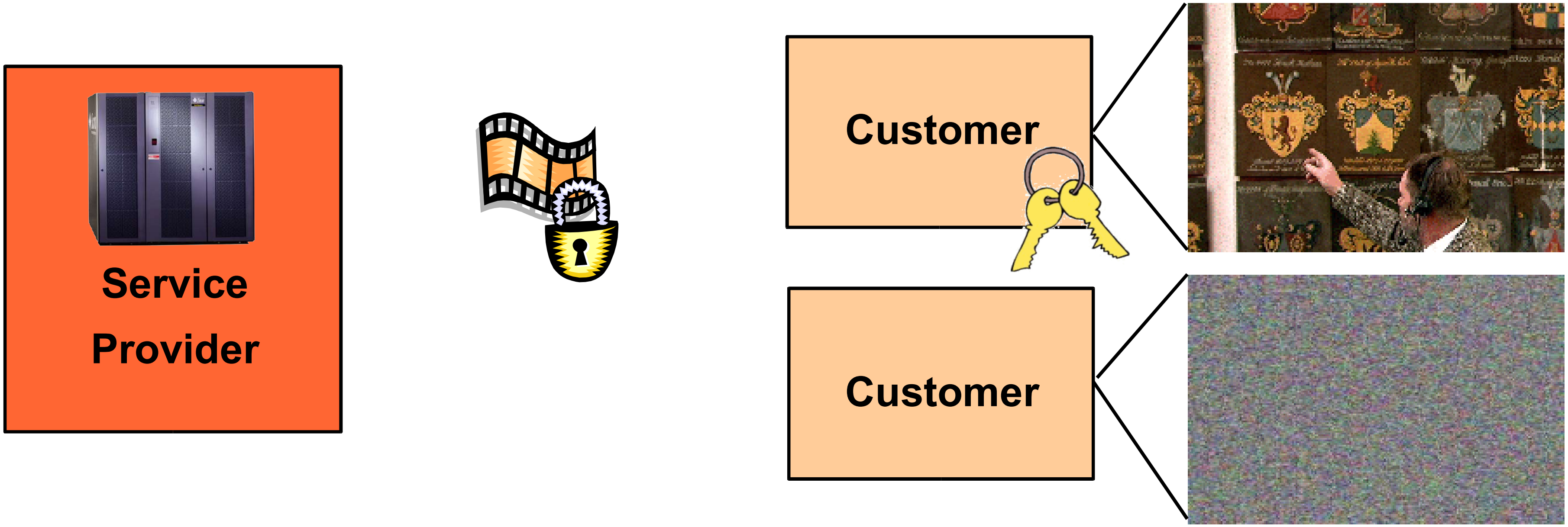
Sebastian Hans
Senior Technical Specialist
Sun Microsystems, Inc.

Kelly Kishore
Researcher
Sun Labs

2008
Sun Labs
Open House

CAS (Conditional Access System)

- A system that controls the access of content through a variety of protection technologies to prevent theft of service.



Service Provider

Customer

Customer

Roadblocks for innovation ...

- Closed specifications / implementations
- Lack of interoperability
- Licensing costs on the Intellectual Property
  - > Specifications may be open but licensing required

Who does this affect?

- Service Providers
  - > Vendor lock-in
  - > New & Innovative services restricted to current vendor capabilities
- Consumer Electronics / Technology Vendors
  - > High licensing costs
  - > Excluded from participation due to closed specifications
- Consumers
  - > Less choices
  - > Higher costs

What is DReaM-CAS?

- Fully specified Conditional Access System for protecting digital TV systems
- Open source / open specifications for industry-wide interoperability
  - > http://openmediacommons.org
  - > https://dream.dev.java.net
- Royalty-free approach to promote boundless adoption and minimize cost-to-market
- Open, robust, and proven security measures to ensure confidence

Telecommunications Act of 1996

- Telecommunications Act of 1996 - section 629 "Competitive Availability of Navigation Devices"
- "... adopt regulations to assure the commercial availability, to consumers ... of ... equipment used ... to access, multichannel video programming and other services ... from manufacturers, retailers, and other vendors not affiliated with any multichannel video programming distributor." - pg 298, subsection(a)
- "The Commission shall not prescribe regulations under subsection(a) which would jeopardize security ... to prevent theft of service." - pg 299, subsection(b)
- "MVPDs must separate out conditional access or security functions from other functions by July 1, 2000 and make available modular security components, also called POD" (point of deployment) - FCC 00-341 9/18/2000
- "The separation of the security element from the host device permits unaffiliated manufacturers, retailers, and other vendors to commercially market host devices while allowing MVPDs to retain control over their system security market host devices" – FCC 05-76 3/17/2005

Currently existing

- CableCARD
  - Closed system with secret security algorithm
  - Licensing fees
- Smart Card
  - Used in Pay-TV for ages but based on proprietary card OS and card application
  - Not aware of open standards defined for CAS card integration and card application
- Downloadable security
  - Proprietary

Roadblocks for innovation revisited ...

- Closed specifications / implementations
- Lack of interoperability
- Intellectual Property
  - > Specifications may be open but licensing required

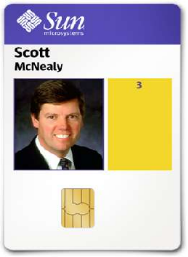
So what does this have to do with Java Card^{TM}?

What is a Java Card ?

- A Secure multi-application platform for a tamper resistant smartcard chip that support
  - Several isolated smartcard applications in the card
  - Load and manage dynamically applications in the card
  - A secure communication of applications in the card
  - To perform complex cryptographic operations
  - To store and manipulate data in non-volatile and volatile memory

Java Card Status

- Over 3.5 Billion cards deployed to date
  - > 825M shipped in 2006
  - > Est. 1.2B shipped in 2007
- Variety of form factors
- All market segments
  - > Telecom (SIM card)
  - > Banking (Payment card)
  - > ID (citizen/corporate card)
  - > PayTV (subscriber card)
  - > Transport, Healthcare...
- 100's of products worldwide



Why a new Java Card Architecture

- Java Card 2.X technology was developed in the late 90 based on the existing technology
  - > IS0 7816 standards maximum 255 bytes of messages
  - > Single threaded application modell
  - > Small memory environment, 8bit CPU
    - Less then 1 KB of RAM, 26-32 KB of EEPROM
- Over the last two years new technology was introduced to the smartcard technology
  - > USB-IC interfaces for high speed communication
  - > Multiple communiation interfaces
  - > Large Ammounts of FLASH memory
  - > 32bit CPU
- Moore's law also applies to smartcard

Technology Drivers

- Take smart card multi-application to the next level
  - Enable applications to execute in parallel over multiple-interfaces
    - Contactless, High Speed interface, ISO interface
- Make the most of the latest hardware capabilities
  - Facilitate usage of large memory cards (multi MB cards)
  - Handle large multimedia files and streaming content (USB)
- Break away from the constraints of the smart card
  - Facilitate smart card integration in a TCP/IP-based network
  - Serve static and dynamic content via standard internet protocols
  - Integrate in webservices infrastructure based on http and xml
- Retain the key attributes of Java Card technology
  - Interoperability, Security, Compactness, Compatibility

Features

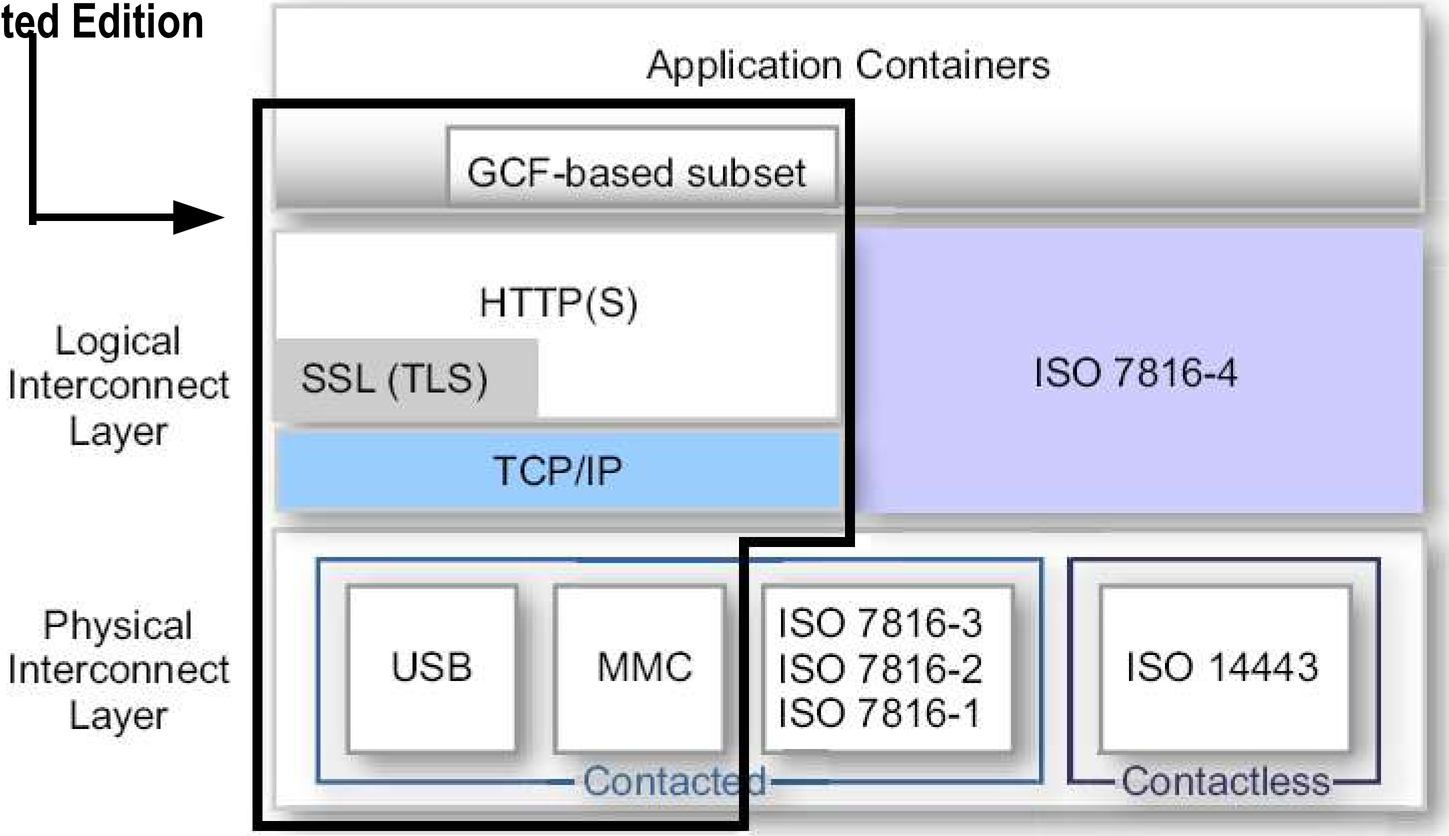
- Smart Card Web Server
  - Provide enhanced end-user experience in Telecom & IT
  - Access card services & user information (SIM book, personalized data) through browser environment
- More capable Runtime Environment
  - support concurrent application execution, more complex Java-types
  - Take advantage of high-end hardware : networked tokens, convergence products (eg: SIM w/ NFC)
- Support for new protocols & memory configurations
  - TCP/IP communication on top of USB or ISO
  - Handle large memory spaces w/diverse security properties
- Streamlined development tool Integration
  - Leverage Java tools and expertise
  - Provide a programming experience consistent with Java ME/SE/EE

Java Card 3.0

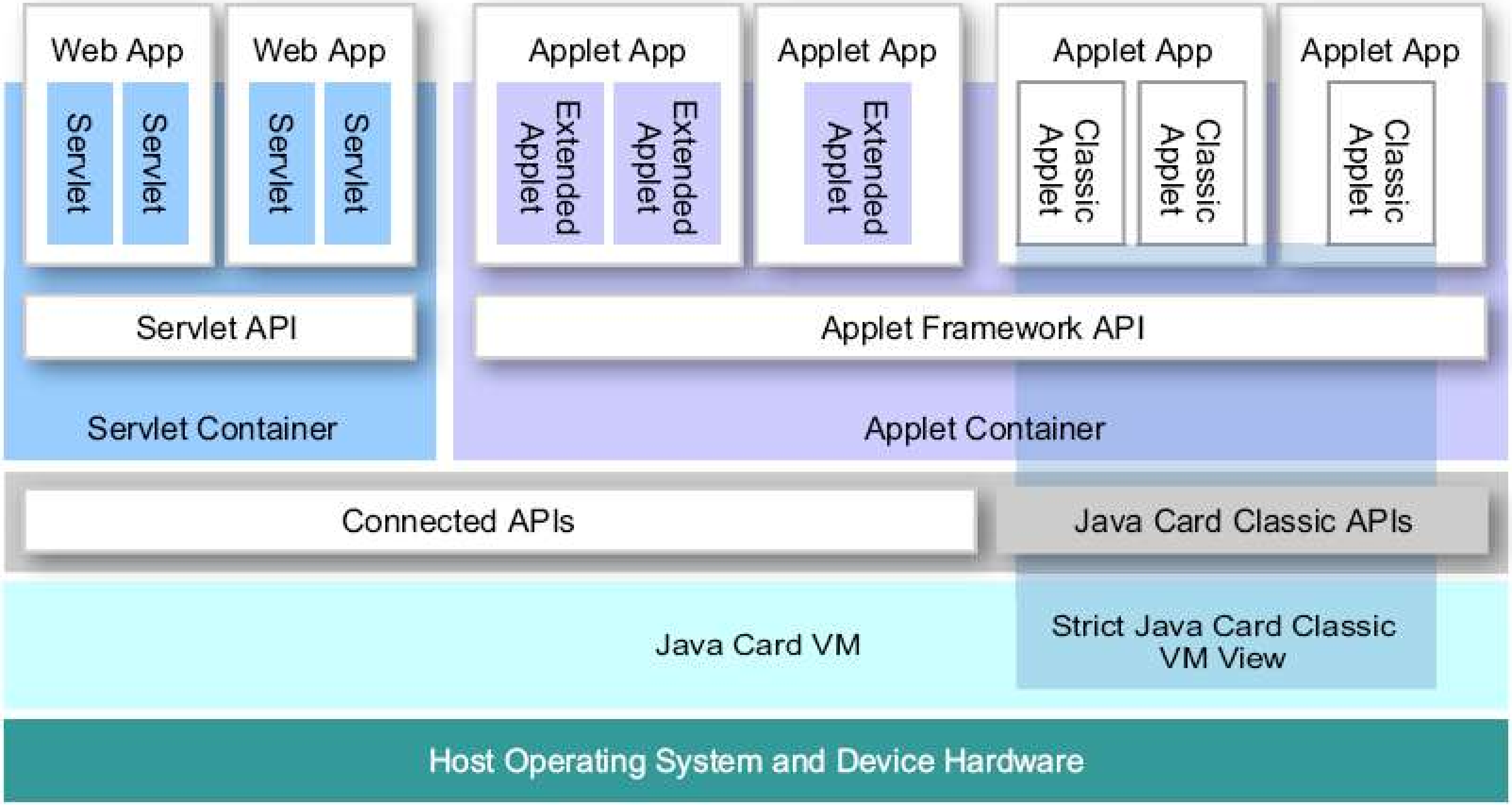
Connectivity Layers and Protocol Stack

New In Java Card 3.0

Connected Edition



Java Card 3.0
High Level Architecture



Programming Model

- Java programming patterns from Java EE and Java ME
- Access to connection-based servlet-like model
  - Can initiate connection-based requests to other servers
- Enhanced Java language features
  - String, Threads, ...
- Richer Utility classes for object management
- Enhanced Sharing and inter-application communication
- Enhanced cryptography toolkit
  - Extensible provider framework
  - SSL/TLS capable

Java Card 3.0 features

- Full backward compatibility
- Multi threaded environment
- Concurrent communication over USB, ISO, contactless interfaces
- Embedded web server with Java Servlet support
- Service static and dynamic content through HTTP (s)
- Client & Server communication mode
- New application models based on Http and TCP/IP communication
- Leverage technology from Java ME and Java EE

Java Alignment

- Java Card 3.0 builds on the strength of the Java Family
  - Reuse existing Java building blocks and tools
- Java Card 2.2.x
  - APDU-based application model and card specific APIs
- Java ME technology
  - Connected Limited Device Configuration (CLDC)
    - Multithreading, Strings, int, long, multi dimensional arrays
  - Generic Connection Framework extension
  - Security Model
- Java Enterprise Edition technologies
  - Java Servlet for web application model

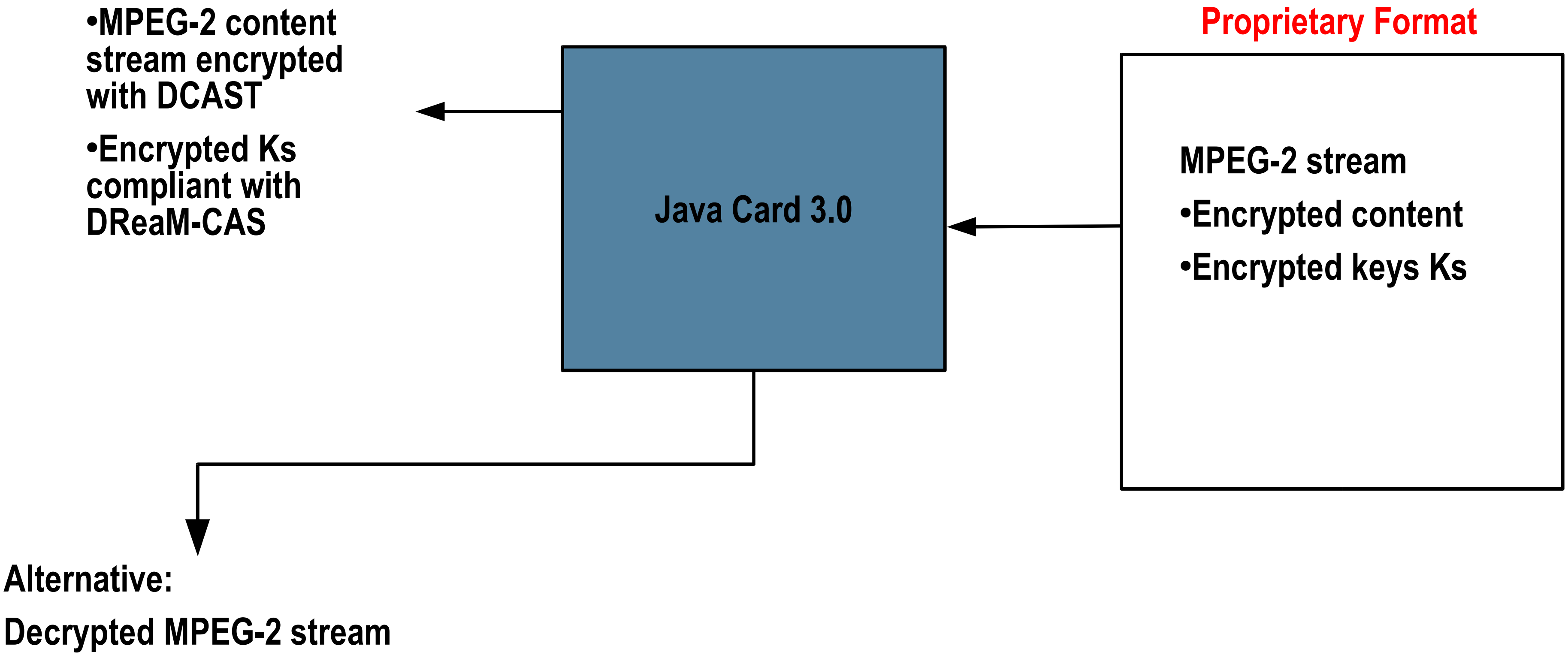
Java Card 3.0 as a platform for CAS applications

- Java Card 3.0 provides the software platform to implement large parts or the entire CAS application and to ease the integration of cards into the device and services
  - It enables the download of such an application over the internet or mobile networks based on open standards
- The next generation of smartcard hardware provides the capabilities to handle large amounts of data
- DReaM-CAS provides the royalty free open standard for a Conditional Access System
- Putting all together provides the complete solution

Java Card 3.0 as a platform for CAS applications

- Java Card 3.0 provide the functionality to implement the CAS subsystem inside the card (DReaM-CAS)
  - CAS application is implemented as Java Card 3.0 application
    - Can be loaded and updated after card issuance
    - Several CAS applications can be hosted in the same card
    - Can be combined with applications for authentication and payment
  - Video stream is streamed encrypted to the card via a secure channel between card and terminal
  - Video stream is decrypted and re-encrypted inside the card
  - Can be implemented on a smartcard with a USB-IC interface or on a card with PCMCIA form factor

High Level Architecture



Proprietary Format

MPEG-2 stream

- •Encrypted content
- •Encrypted keys Ks

Java Card 3.0

- •MPEG-2 content stream encrypted with DCAST
- •Encrypted Ks compliant with DReaM-CAS

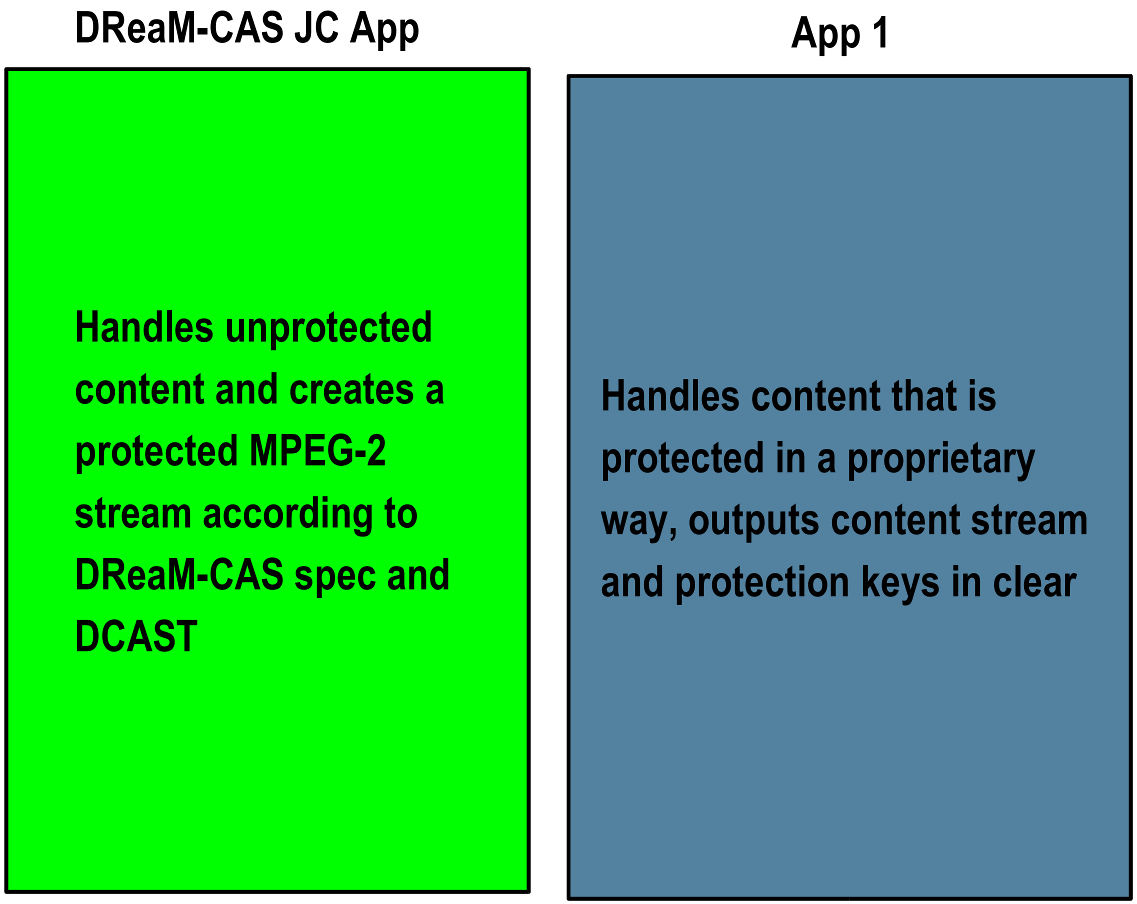
Alternative:

Decrypted MPEG-2 stream

Internal Architecture

- MPEG-2 content stream encrypted with DCAST
- Encrypted Ks compliant with DReaM CAS

Keys Ka in a secure container compliant with DReaM-CAS



DReaM-CAS JC App

Handles unprotected content and creates a protected MPEG-2 stream according to DReaM-CAS spec and DCAST

App 1

Handles content that is protected in a proprietary way, outputs content stream and protection keys in clear

MPEG-2 stream
- Encrypted Content
- Encrypted keys Ks

Keys Ka in a secure container

The DReaM-CAS JC App will provide an interface to application s of type 1 to receive their output

Java Card enables the loading of App 1, there can several app of type 1 in the card to enable different types of content protection

Thank you