

Security Architectures in Mobile Integrated Pay-TV Conditional Access System

Hamidreza Shirazi

Hamidreza.shirazi@brunel.ac.uk

Research Engineer

Brunel University, UK

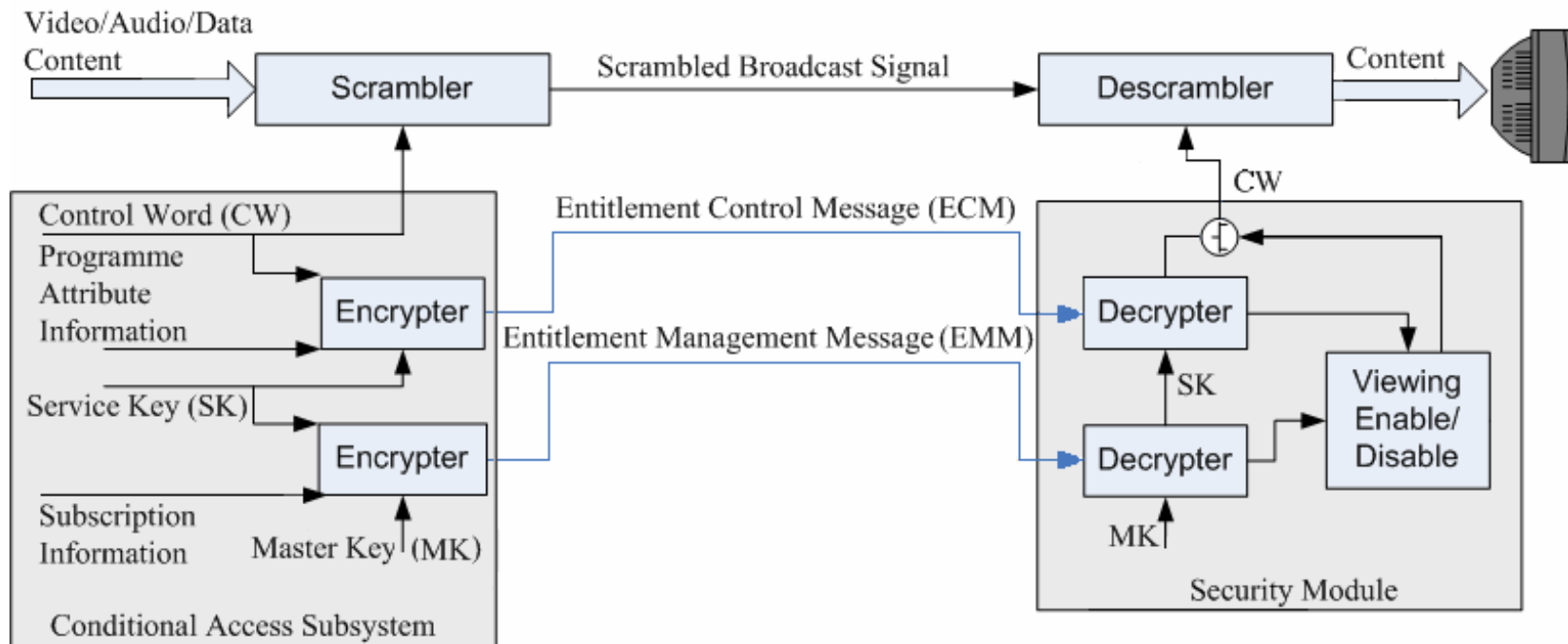
Strategy & Technology Ltd., UK

Agenda

- Existing Conditional Access (CA) system
 - Typical Pay-TV CA system
 - System structure
 - Problem statement
- Proposed Conditional Access system
 - General system model
 - New entities and required APIs
 - Security structures
- Conclusions & future works

Typical Pay-TV Conditional Access (CA) system

- CA system is applied in Pay-TV to help service providers to control users' authorisation by
 - Scrambling signals to prevent non-subscribers from receiving it;
 - Processing access control messages to determine if descrambling is to be performed.



Problem statement

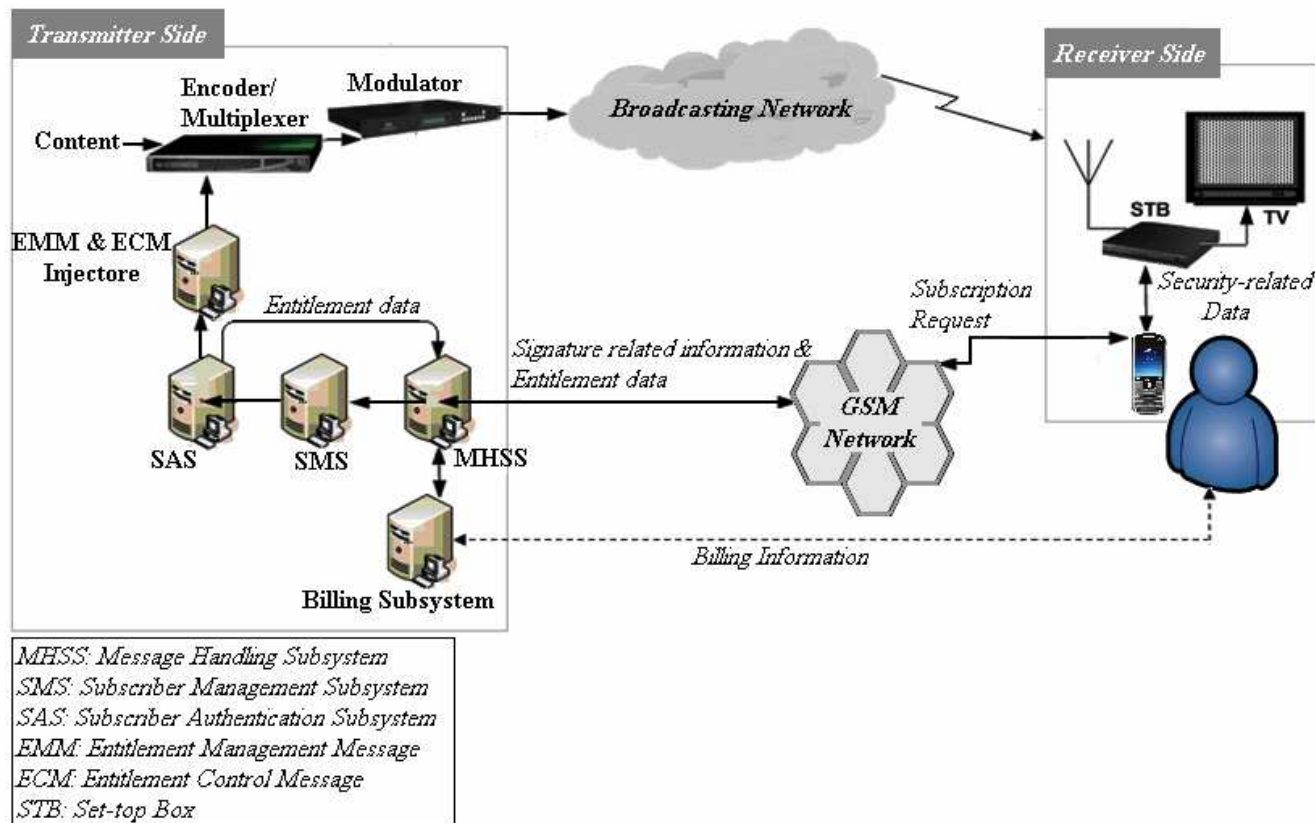
- Vertical transaction model where service provider, CA provider and STB producer are bound together
 - Commercial loss for STB producers
 - Slowing down the technology enhancement and competition
 - Expensive STBs
 - Subsidiary package to attract potential customers
 - Interoperability issue amongst service providers
 - DVB Simulcrypt and Multicrypt protocols
 - Software downloading technique
 - PC or Common Smart-Card based CA system
- High cost of operation & service deployment
- CA messages are broadcast to all receivers
 - Security issue
 - Complexity
 - Bandwidth usage
- Lack of interaction
 - Limited security and functionality management
 - No personalisation
 - Java Card technology
- Imposing pre-determined STBs to subscribers
 - Compromising subscriber's freedom of choice over STBs
 - Stack of STBs

Solution statement

- A platform is needed to allow
 - Service providers to deploy their tailored CA system
 - Service providers to automatically detect piracy and revoke compromised Key in the system
 - Service providers to study on their subscribers' behaviour and come up with more targeted and personalised offers
 - Service providers to change or update their security platform cost effectively as and when it is needed
 - New rivals and entrepreneurs to enter to the market and operate easily
 - Service providers co-exist at both head-end and receiver-end
 - An amalgam of SIMULCRYPT and MULTICRYPT protocols
 - Subscribers to freely chose and switch between service providers who are operating in a specific geographical area
 - Subscribers to freely chose their own set-top boxes
 - Subscribers to manage their subscription and enjoy their entitlements more freely via an arbitrary receivers

System model

- System model of Mobile Integrated Conditional Access System (MICAS)
 - Message Handling Subsystem
 - Underlying agents (APIs)

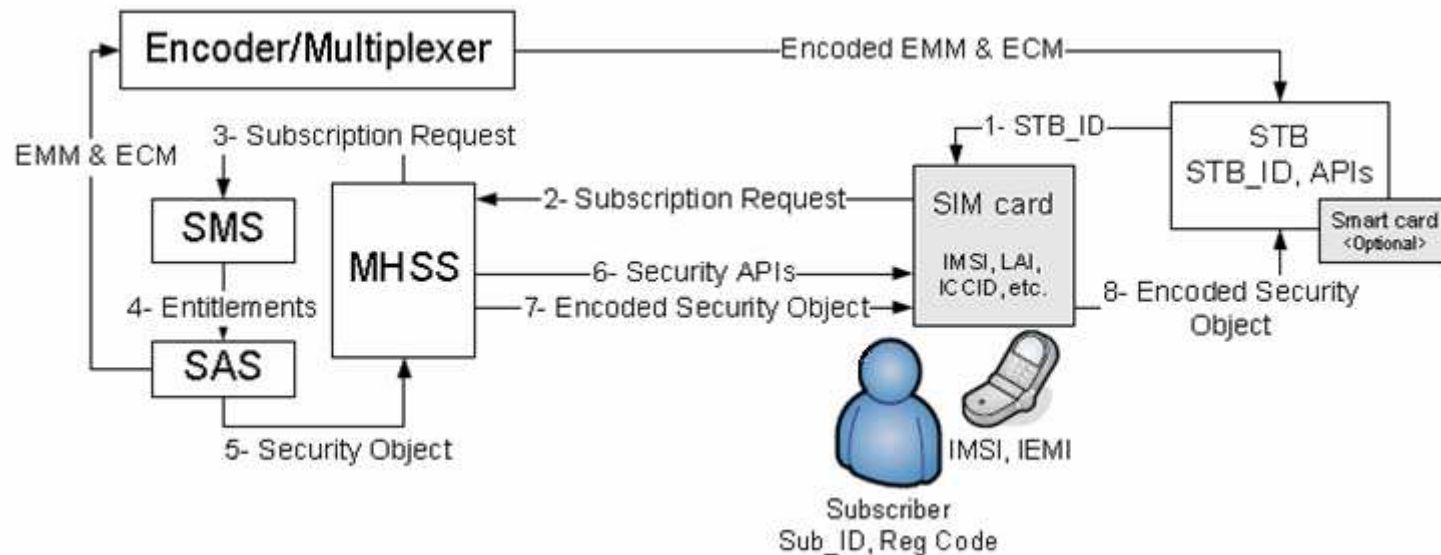


- Message Handling Subsystem (MHSS) mainly:
 - Acts as an interface between head-end and subscriber in GSM network
 - Receives the subscription requests
 - Performs authorisation and authentication processes
 - Verify the request issuer
 - Subscriber
 - Mobile phone
 - Set-top box
 - Evaluate the security status of the client and performs security update (i.e. Bootloader update) and remote installation
 - Forwards the requests to the Subscriber Management Subsystem (SMS) for access provisioning
 - Instructs the billing subsystem to proceed with payment authorisation

- Underlying agents/APIs:
 - Subscription Request Handler
 - A MidLet running on the mobile phone (or STB):
 - Present Electronic Service Guide (ESG) or Electronic Programme Guide (EPG)
 - Generates and sends the subscription request
 - Performs mutual authentication processes between mobile phone and set-top box, and mobile phone and MHSS
 - Conditional Access (CA) Handler
 - An Applet running on the SIM card inserted in the mobile phone
 - Downloaded and updated by the MHSS
 - Performs security sensitive functions to control the access to contents
 - Generates and sends an authorisation message to the MHSS to verify the subscription request issuer
 - The authorisation message may include the International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI) and Set-top Box ID (STB_ID)
 - Communication Daemon
 - An embedded application running on the STB
 - Provides a secure link between the STB and mobile phone
 - Performs the pairing sequence between the STB and mobile phone
 - Handles data exchanged with the mobile phone for instance through the Bluetooth channel
 - Transfers the set-top box identifier to the CA Handler

Security architectures

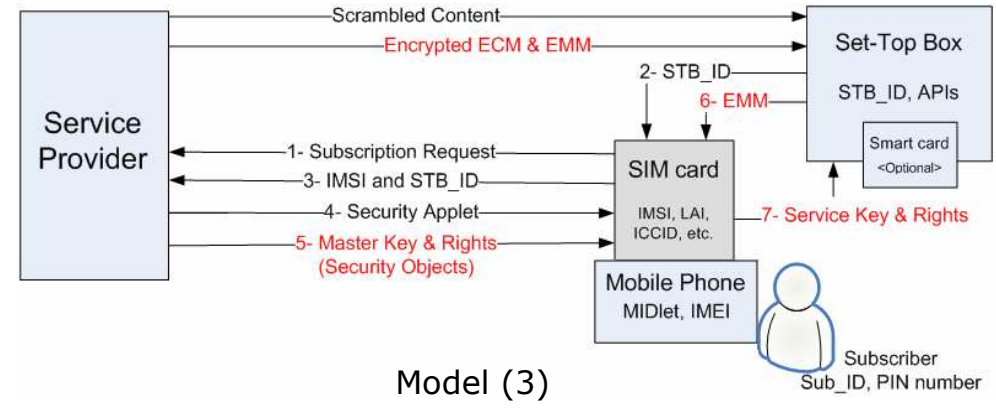
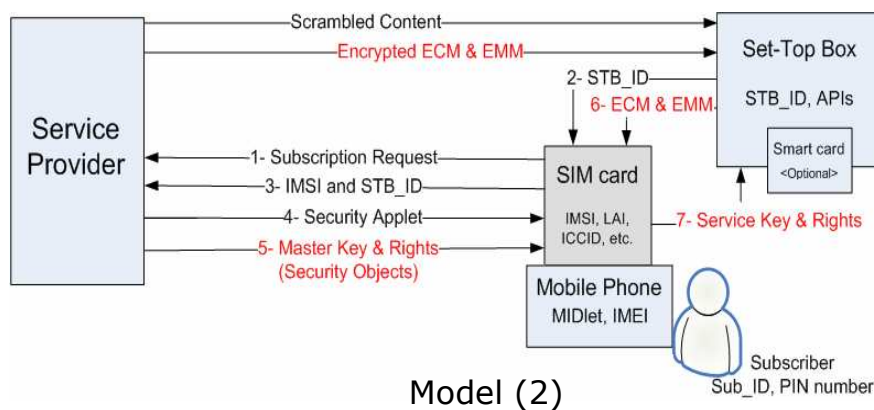
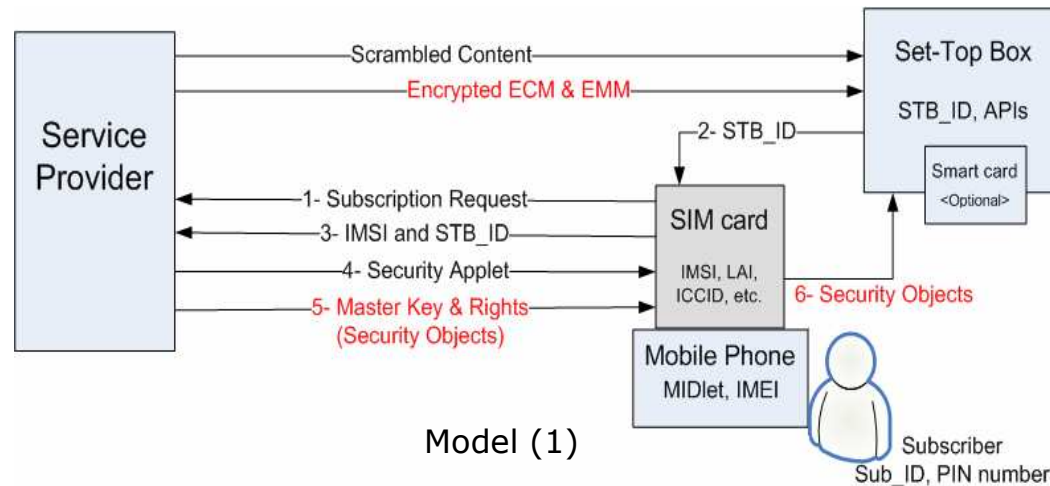
- Various security architectures can be introduced depending on
 - Key hierarchical system
 - 3-level Key hierarchical system: Master Key + Service Key + Control Words
 - 2-level Key hierarchical system: Service Key + Control Words
 - The security data sent over the Broadcasting medium and GSM network
 - Security data is referred to the Security Object and CA messages (EMM and ECM)
 - The location wherein the security data are processed
 - Either in the set-top box or mobile phone



Security architectures

Cont.

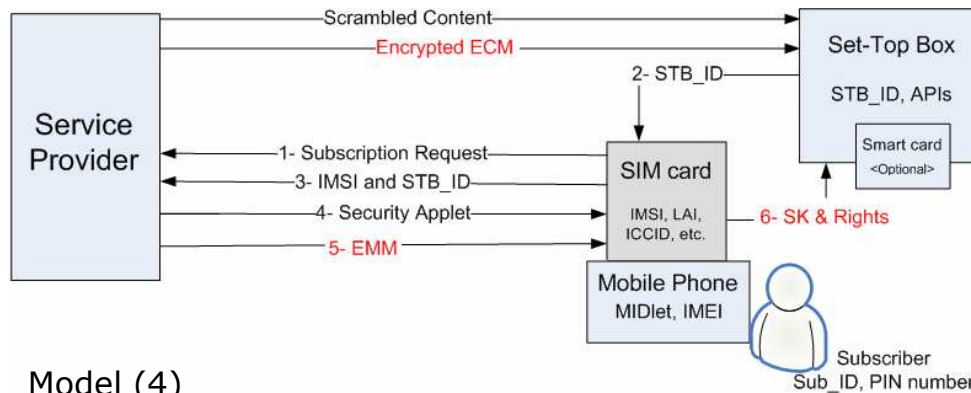
- Security models based upon the 3-level Key hierarchical system – EMM & ECM are delivered via Broadcasting medium



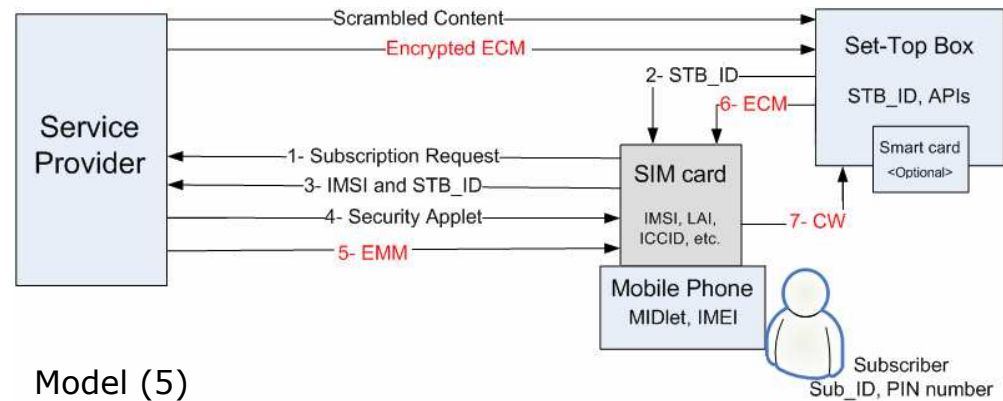
Security architectures

Cont.

- Security models based upon the 3-level Key hierarchical system – ECM is delivered via Broadcasting medium and EMM from GSM network



Model (4)

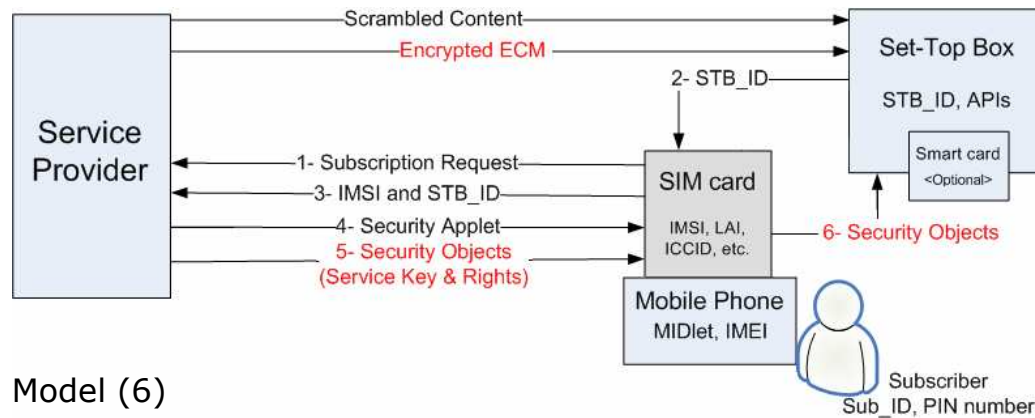


Model (5)

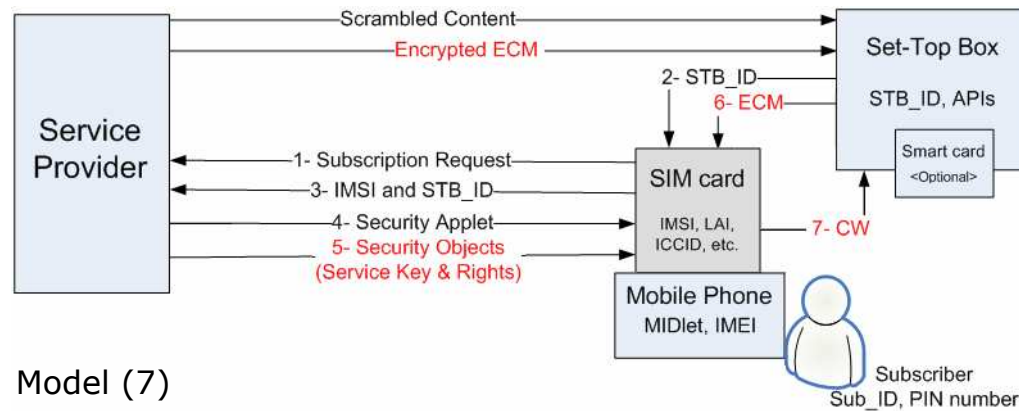
Security architectures

Cont.

- Security models based upon the 2-level Key hierarchical system – ECM is delivered via Broadcasting medium and EMM from GSM network



Model (6)



Model (7)

Security architectures

Cont.

- Common aspects in explained security architectures:
 - The smart card is optional in the STB implementing a CA system
 - Mobile phone can be replaced with any device with similar features in mobility, security and storage
 - All interaction including downloading, revoking or updating new security algorithms and Keys can be done via GSM network
 - Security techniques like encryption, session management, digital signature, mutual authentication, etc can improve security in all interaction courses
 - Service provider can monitor subscriber's contractual behaviour for preventing any piracy and offering more personalised services
 - The "Follow-Me" service can be offered in all the security models
 - Follow-Me would enable the subscribers to enjoy their entitlements through any arbitrary set-top box.
 - A step to break the rigid one-to-one relationship between a subscriber and set-top box currently imposed by the service provider

Conclusion & Future works

- ✓ A typical model of the CA system was explained
- ✓ Current issues in the legacy Pay-TV system was highlighted
- ✓ A solution was modelled to integrate mobile technology in the broadcasting system
 - Mobile Integrated Conditional Access System (MICAS)
- ✓ Various security architectures were modelled based upon:
 - Delivery method of CA messages (EMM & ECM), processing location and hierarchical Key system
- ✓ The MICAS is considered as a solution for:
 - Provisioning horizontal market and interoperability in Pay-TV
 - Reducing service deployment and compromised Key replacement costs
 - On-line installation and key revoking mechanism
 - Offering more affordable products
 - Offering higher security and wider range of bespoke services
 - Offering Follow-me type of services to subscribers
- **Future works**
 - Thorough analysis of each security architecture in terms of security, performance and other functional and non-functional requirements
 - Simulating the system and investigating the effect of the GSM network on the system
 - Prototyping a more viable model
 - Possibly being involved in a bigger European project to use the MICAS model for implementing a Federated Identity solution across the converged telecom and broadcasting systems

QA ?!

Thanks for your attention