



# Secure delivery of personal TV and video content

**NOKIA**  
Nseries

# Television redefined

Three major underlying trends in today's media are digitalization, networking and mobility. Media content is becoming digital. Media delivery devices and – most importantly – media users are getting networked with each other. Users are mobile, and their media consumption is to take place on the move.

Digitalization, networking and mobility lead to development of new products and services that people are willing to pay for. On the other hand these trends also give consumers choice and power – in the digital world people are not tied with single proprietary concepts in their communications or media use. The most notifiable example of this is the power of the Internet, peer-to-peer communications and user-generated content that can seriously challenge the foundation of the traditional media business.

Television viewing is changing as well. Digital transmissions provide people a growing supply of television content, a trend that also leads to fragmentation of TV audiences and challenges for the advertisement funded business models. New time-shifting and place-shifting devices such as DVRs give viewers the option to watch their favorite programs when they want – and skip the ad breaks. IP based video delivery paves the way for new TV business models but also fosters the spreading of illegally copied content.

Mobile communications have already changed the way people communicate with each other. Telephone used to be a device associated with a single site, e.g. house. The development of digital mobile telephony not only made the telephone device mobile, it also facilitated the emergence of the concept of personal communications device. On one hand, the mobile devices have provided novel ways for one-to-one communications; on the other hand people can enjoy the services of personal tools such as calendar and notebook they can use with their mobile devices.

Growing data rates in cellular networks and the launch of DVB-H based mobile broadcasting services now make the viewing of high-quality TV and video content on mobile devices a reality. Even WLAN networks can potentially be used for TV and video delivery. We will be witnessing the same development as what happened to telephony: television viewing will become not only mobile, but also personal.

### Implications for business models

In the TV industry, for the advertisement-funded free-to-air (FTA) business model no significant growth is expected due to the challenges deriving from e.g. audience fragmentation and time-shifting devices. However, despite the

moderate growth the FTA business model will continue to play a role in the future as well. Pay-TV business is expected to enjoy a total growth of 76% during this decade, reaching USD 173 billion in 2010 (Informa).

In addition to these two basic business models we will see new ways of monetizing TV and video content, such as digital download and video-on-demand services. In a wider context, TV advertising will potentially converge with e-commerce services and CRM activities.

Most commonly the pay-TV content costs the viewers a monthly fee. In some cases the pay channels are bundled with TV or Internet access charges. Digital video download and video-on-demand services may be offered for either a one-time charge or as a subscription package. TV operators may also offer some video-on-demand content for free as a churn-reducing measure. The on-demand services may provide the user a one-time access to the content (e.g. streaming) or the full ownership (downloading).

In mobile TV the content may be transmitted as broadcast, streamed or downloaded. The downloading can take place real-time or as a background activity. For each way of content delivery, appropriate transmission technologies are used. The technologies should be transparent for the viewer, who is only interested in the content.

Mobile broadcast TV services are in most cases offered as a bundle, which comprises both the access of mobile TV services and a number of free-to-air or pay-TV channels. Three potential mobile TV business models are explained below:

- **Wholesale model**, where Broadcast Network Operators will, in addition to building and operating the DVB-H network, expand their pure network operator role and take an active role in aggregating the mobile TV service portfolio. Wholesaler then offers this service portfolio to mobile operators, who act as service reseller and sell the service to their customers. Service reseller takes care of marketing, customer care and billing. Service reseller and wholesaler work on a revenue sharing basis. As a variation of the wholesale model broadcast network operator may sell a part of its DVB-H network capacity directly to mobile operators, who can utilize the capacity to distribute exclusive content to their customers. This allows them to better differentiate their service proposition from competitors. Another variation of this model is that wholesaler sells a part of the capacity directly to broadcasters, who may offer their services either free-to-air to consumers or pay-TV services making reseller agreements with mobile operators.



Content type	TV & Video	Music	Applications	Internet
Bearer				
DVB-H				
Cellular (GSM, EDGE, WCDMA)				
WLAN				
Memory cards				
PC connectivity				



**Mobile TV handsets must handle DRM for all content types over all distribution methods**

• **Mobile operator driven model**, where Mobile Operators aggregate their own mobile TV service portfolio by making deals with TV channels and content owners. Mobile operators then sell the service to their customers. Typically mobile operators don't build and operate their own DVB-H networks. DVB-H networks are normally built by separate companies, DVB-H broadcast network operators. DVB-H network operators rent the network capacity to service operators, i.e. mobile operators, so mobile operators act as virtual broadcast network operators. In the most cases, DVB-H network operator and mobile operator have a long-term, fixed-fee contract for the capacity.

• **Broadcaster driven model**, where Broadcasters acquire capacity from the network operator and offer the services directly to the consumer. This model is the most likely one, if mobile TV services are offered free-to-air, but the model naturally allows also pay TV services. The mobile operator may have a role in CRM and interactions, but more from a subcontractor role or position.

**Securing the content**

A necessary bedrock for mobile TV and video business is that the content creators, aggregators and operators can choose – based on their business model – how the content is charged for and what kind of viewing and redelivery rights are associated with the charge. Equally important is that those companies can trust in that their content is delivered and used in the way they have chosen.

The multitude of potential business models will grow and mobile TV infrastructure needs to support a multitude of options, how to charge for and in which ways to deliver the content. Where one content owner would strictly only allow one-time viewing of its content, another may want a piece of a content to be spread to a maximum number of viewers for promotion purposes.

Also the variety of ways to transmit the media content to the users – including e.g. cellular, broadcast and WLAN networks – leads to the requirement that the content security technologies need to be carrier agnostic.

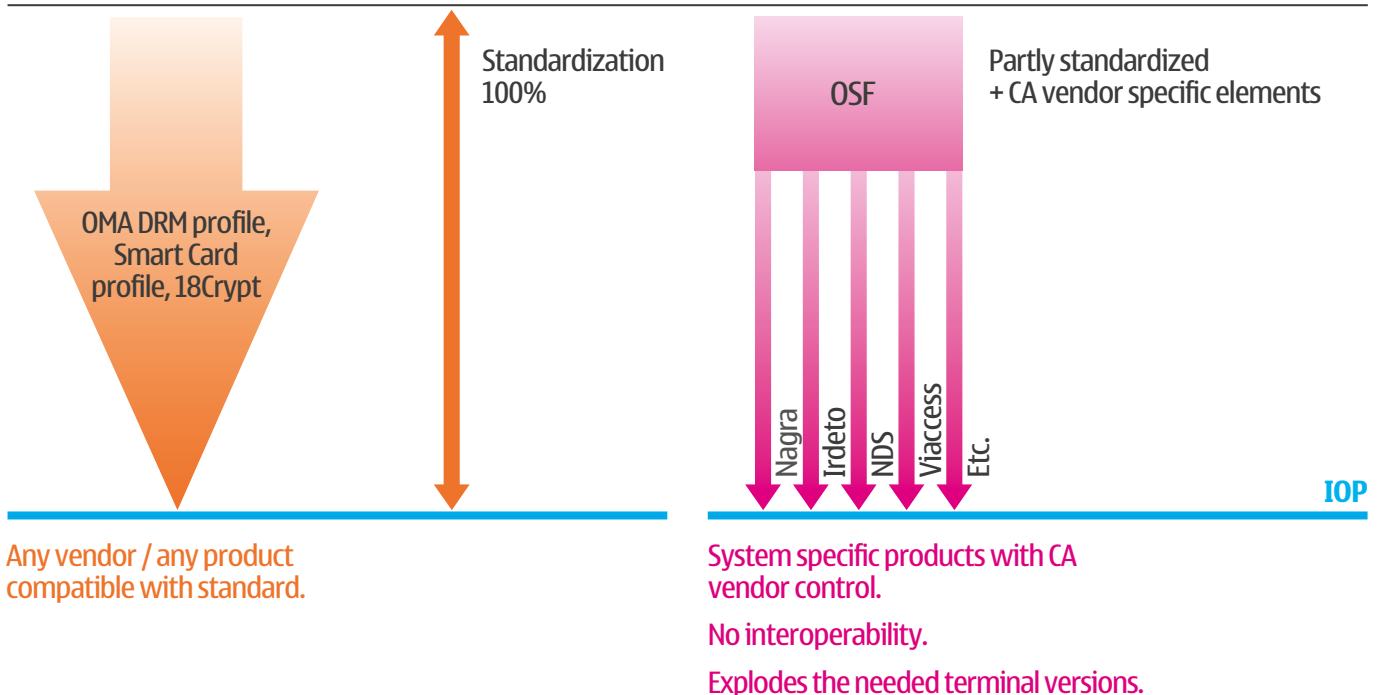
In the traditional pay-TV world the securing of the content is based on a concept of conditional access (CA). CA regulates literally whether a viewer has the rights to access a TV stream. Typically a CA system is implemented with a system specific embedded SW inside a terminal and with a chip card that is inserted in a card slot in the TV receiver. Conditional access is

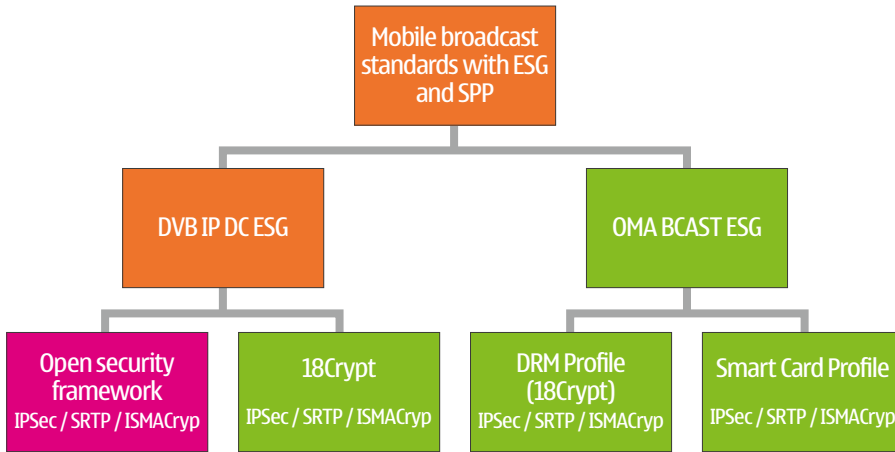
a satisfactory concept for securing linear TV content. However, once the viewer has received and possibly recorded a piece of content, the CA system can no more control the reuse of the recorded content. In other words, conditional access suits for traditional fixed-location pay-TV business models, whereas the requirements set by new business models call for other approaches for securing the content.

In cellular networks solutions already exist for protecting media content. OMA DRM 1.0 (Open Mobile Alliance Digital Right Management) is the industry standard for protecting a wide range of services, ringtones, logos and even short video clips. OMA DRM currently protects mobile content business worth of hundreds of millions of dollars annually. To better match the enhanced needs of the DRM adopters and users, OMA has further developed their DRM specification. Among the key features of the new OMA DRM 2.0 are teasers/preview, superdistribution and enhanced security level of the system.

The model used in traditional TV service protection, allow for partly standardized systems and the room left for CA vendor specific implementations leads to market fragmentation. This way of thinking has been used when defining the OSF system. Unfortunately the use of proprietary systems in telecom environment has not proven to be beneficial to any business player. If a proprietary method for Service Purchase and Protection, (SPP) would be widely taken into use, the number of needed terminal versions will explode exponentially. The end customer will eventually pay for all additional costs. Let it then be terminal or system costs.

OMA BCAST specified service purchase and protection systems together with 18Crypt represent a flexible, network-agnostic, future-proof solution for the content security needs of mobile TV business.





**ESG and service protection standards**

**Service purchase and protection**

Two organizations have developed SPP solutions for Mobile TV: DVB and OMA. They may have looked the needs from different perspectives, but have accepted one common element: The 18Crypt and OMA DRM Profiles are almost identical. OMA BCAST has specified the systems to be bearer agnostic so that they can be used for all types of Mobile TV. The Smart Card profile is compatible with MBMS security and it is made mandatory for terminals having mobile interactivity channel.

In streamed content protection OMA DRM 2.0 is complemented by service purchase and protection (SPP) technology called 18Crypt (OMA BCAST uses term DRM Profile). Secrets management of 18Crypt is based on OMA DRM 2.0.

The OMA DRM Profile is a service purchase and protection standard optimized for broadcast media. 18Crypt has been developed by major industry players representing broadcasters,

mobile network operators, component manufacturers, security companies and terminal vendors and it has been approved as a standard by ETSI and IEC.

The OMA DRM Profile can be used for protecting transmission phase of any kind of IP based content ranging from ring tones to video clips. The same technology can be applied for content protection to protect the content after the transmission.

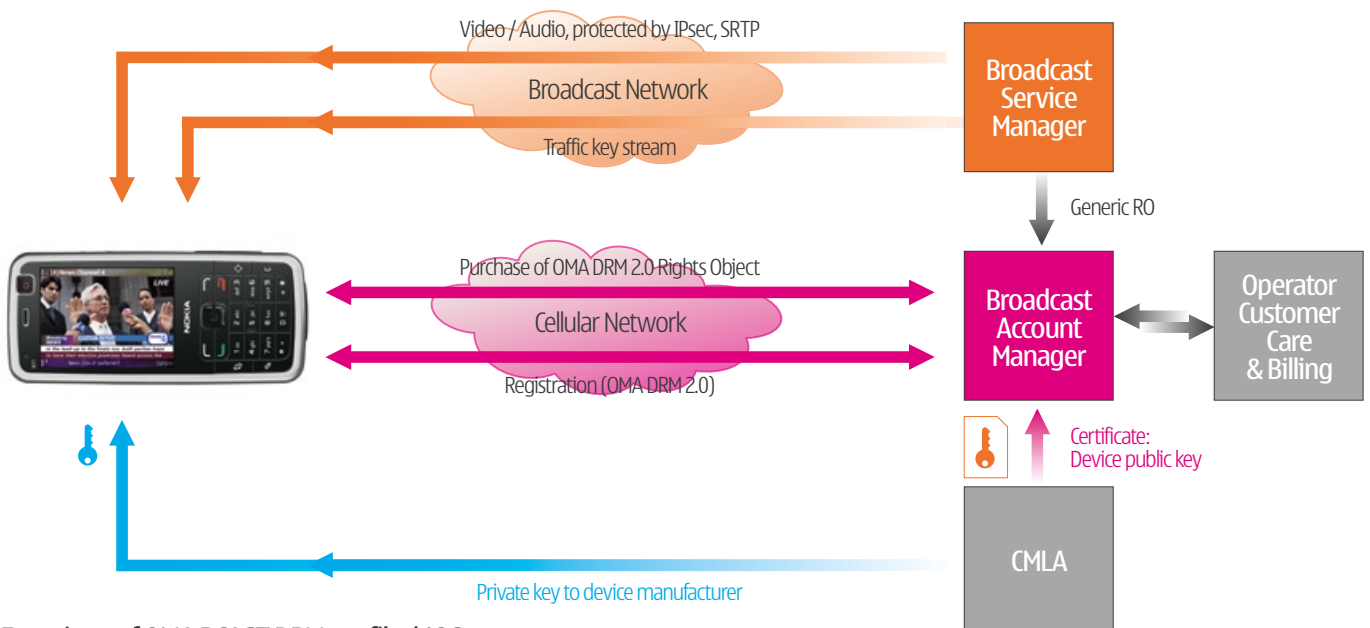
The memory capacity of all terminal devices is growing rapidly. This means that more and more content will be stored in the terminal. The combination of OMA DRM 2.0 with Service Purchase and Protection methods supports media consumption from all sources with a cellular device. By using one and the same system for all DRM functions makes terminal users' life easier. Ease of use and familiar mechanisms encourage users to further increase media consumption.

The new Nokia terminals offering gigabytes of memory capacity provide suitable platform for enjoying media protected by OMA DRM 2.0 for content protection and mobile TV SPP. The user only needs to learn one user interface for all purchase actions. This will generate more transactions when the user reaches comfort zone much faster.

For an operator, combining DRM and SPP technologies give cost savings, shortens the learning curve and makes the usage of the services easier to adopt.

The OMA BCAST specified profiles and 18Crypt offer all purchase methods that are used in traditional pay-TV business, such as:

- Subscription based, with variable subscription time. If no timely restriction is needed, then the subscription may be open ended and the termination will be taken care of when requested.
- Program based. The access is limited to one selected program.



**Functions of OMA BCAST DRM profile / 18Crypt**

- Event based. Access is limited to an event. An example would be a bundle of services of a sports event.
- Pay per view. The purchase may be based on time or use of tokens.
- Preview. The user can access a limited period of the beginning of the program. This can be done by granting definite length (e.g. 5 minutes) access rights to the service.

As the keys are protected with OMA DRM 2.0 (DRM profile and 18Crypt), additional business options are possible using advanced features of OMA DRM 2.0 technology: Examples of such are superdistribution, preview of services and access rights buying to a friend.

**Requirements for a mobile TV SPP system and how the fully standardized SPP solutions meet them**

A Service Purchase and Protection system has both technical and commercial requirements set by consumers, Mobile Network operators, Broadcasters as well as Content owners. All those requirements need to be addressed and fulfilled by the system that was selected to be used with Nokia terminals.

**• Security**

The system must provide security level that is approved by all partners in the Mobile TV ecosystem.

The DRM profile has been designed to use state of the art algorithms for both service encryption as well as for Key System security. It has been designed with security experts to facilitate a proven concept.

**• Horizontal markets**

A horizontal market is a must for all new systems. Horizontal markets catalyst fast growth for new services as well as bring rapidly the costs down for system components.

The systems have been standardized completely. They do not contain any proprietary elements thus making independent, interoperable implementations possible. They have a Trust Model that is provided by an external organization thus freeing the system users from single vendor lock in.

**• Interoperability between terminals and networks**

The success and future-proofness of any system requires that there are several equipment vendors present with products. And those products need to be interoperable to complete a success story.

The systems are designed for interoperability. All elements of the specification are available and public information. There are currently several system providers for the technology, both for head ends as well as for terminals.

**• Roaming of terminals and services**

Any user of a mobile device is used to have access to different services – also when not in their home network area. Providing services to visiting customers is potentially a big business. This is true as long as terminals and services can roam and are not locked to a proprietary system.

The standardized systems base their roaming to several technical measures:

- a) All terminals follow the one and same standard,
- b) All Broadcast systems follow the same standard
- c) Roaming is a key element of the specification. It has been designed to follow the roaming mechanisms currently used for mobile voice and data services.

**• Need to enable versatile usage models: A/V, Filecasting**

The need for datacasting, not only TV services have been known from day one of Mobile broadcasting. There is a growing user demand for additional services, music, ring tones, SW applications etc. Any system that will be used for Service Protection must provide a mechanism to protect also those services.

One of the encryption methods defined for the Smart Card Profile, DRM Profile and 18Crypt is IPsec. It can be used for all IP based content and it provides a secure bit pipe for transmitted content. In case an additional Digital Rights Management system is used, IPsec does not limit the choice of the system.. The DRM profile and 18Crypt use OMA DRM 2.0 for Key Messages. A natural choice is to use that also for content protection.

**• Renewability**

No system is secure for an indefinite time. Therefore the selected system needs to be renewable in case a system upgrade is needed.

There will be no identical system implementation. The selected algorithms are secure as of today but need to be renewed when the security may be endangered. Upgrading a standard can and will be done before the security is risked. The industry is committed for that.

What comes to terminal renewability, there is currently an OMA standardized mechanism that can and will be used for terminal software upgrades. Those upgrades can be forced to take place and can happen either over the mobile network or via Internet.

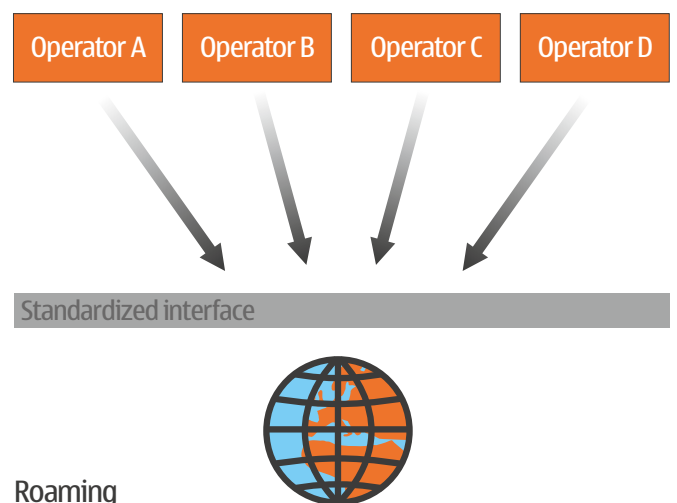
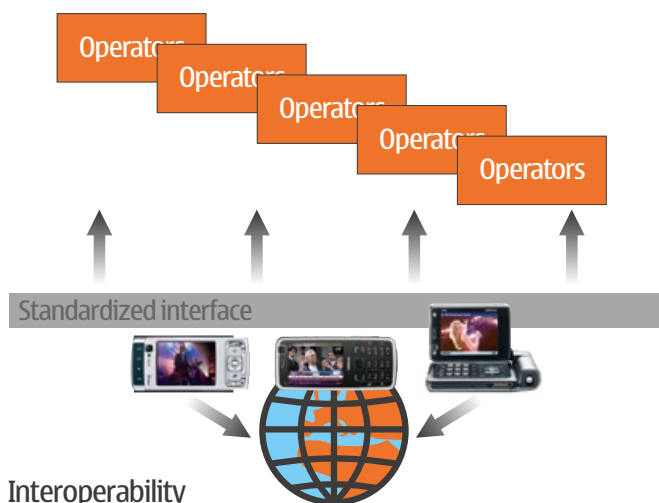
**Interoperability and roaming**

Standardized, open interfaces will enable manufacturers to produce products compatible with the standard as soon as there is business potential. It will enable fast growth of businesses as well as competition between products from day one usage. This leads to a status where price for the customer is always optimum and generates market interest, which in turn enables fast market growth and scale of economics.

This is also the case when applying OMA DRM, OMA SPP profiles and 18Crypt for mobile TV and video content security.

A standard that is fully specified and leaves no room for variations gives a solid base for interoperable products. Service systems and terminals will interoperate without a compromise in system performance. Thus there is no need for multiple streams for content or key deliveries.

Standard products not only enable interoperability and competition, but also open potential for various business models with easy to see benefits. A good example of the benefits and advantages of an open and standardized system is the fast and successful deployment of GSM standard and products based on it.



An important, often forgotten aspect of mobile TV is roaming. It is also a key to additional business. Mobile TV users expect that their devices work not only in their home network, but also when they travel. They do not expect to get their home content, but to get access to Clear-to-Air (CTA), Free-to-Air (FTA) and encrypted services.

Additional revenues are available for operators offering easy access to services like sports events or international news services also for visiting customers. A fully standardized solution offers the same air interface between terminal and visited network as is in the customer home network. There is no need to bother the customer with complex technical procedures of how to acquire the access to the visited network, as is the case with proprietary conditional access service protection solutions. The standard air interface enables building roaming function as long as mobile network operators have an agreement that allows service roaming.

**Security solution**

OMA has specified digital rights management solutions, referred to as OMA DRM 1.0 and 2.0. Secrets management of the DRM Profile and 18Crypt uses OMA DRM 2.0 technology. OMA DRM 2.0 specified Rights Objects (RO) are used to deliver keys and entitlements.

The security of the DRM Profile and 18Crypt is based on AES-128 and RSA algorithms, perhaps the best understood and widely used ones in the security industry. Many of the e-banking systems today rely on AES-128 and RSA algorithms. The key lengths have been selected to provide optimal terminal performance and security. The rival SPP solutions for mobile TV are expected to use these same algorithms.

AES-128 as an algorithm has been qualified by NSA (National Security Agency) for US Government classified information.

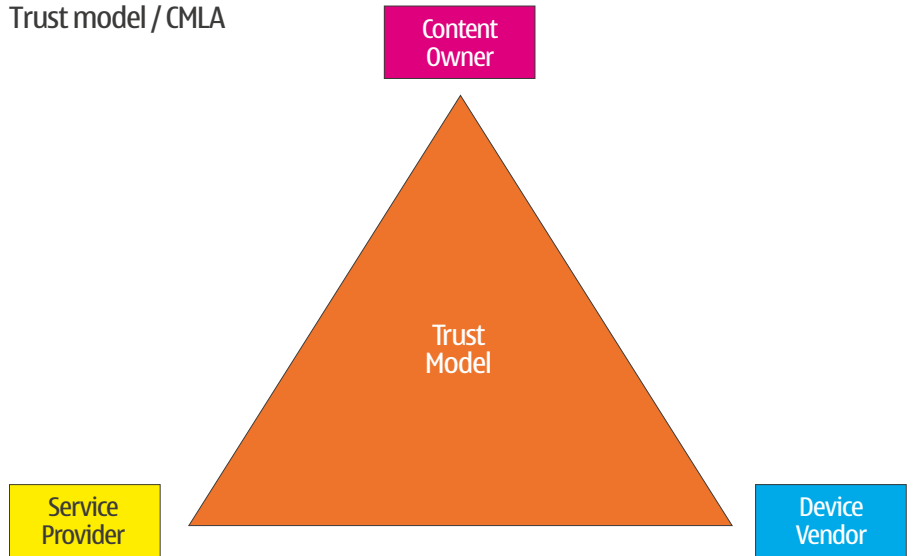
When selecting which methods to use, one of the key validation points was to ensure future-proofness and versatility of services to protect. The selected system should be possible to be used in IPv6 or IPv4 networks and enable protection to all imagined content to be transmitted over the broadcast network.

IPSec guarantees that any content delivered on IP could be encrypted. I.e. it is fully content agnostic. There are no limitations to the content format, DRM system used, or to modes of operation. In addition to IPSec, also SRTP (Secure Real-time Transport Protocol) and ISMACryp may be used. While IPSec provides merely protection for service delivery, SRTP can also be used to protect stored content.

IPSec is a basic element of any IP stack implementation of an IP receiver, and SRTP is a mandatory element of 3G devices. Therefore they do not generate a need for any additional SW components.

All elements of the DRM profile (and 18Crypt) are standardized, but the ways to implement those elements will differ. The selected encryption algorithms have been in use for

**Trust model / CMLA**



years or even decades, and are widely deployed in other commercial solutions. Therefore the requirement of renewability is primarily on implementations, not on the standard still maintaining the interoperability.

There are several ways terminal system software can be upgraded in the field. The Nokia N92 and N77 will use an OMA standardized FOTA system to enable system software upgrades. The upgrade can be limited to sections of software or to cover the full software thus offering flexible system upgrades.

The Nokia terminal SW update mechanism checks that the origin and the source of the new SW are only the approved ones. (The check is based on asymmetric algorithms and public key technique, which enable terminal software integrity & authenticity verification for Nokia mobile terminals against illegal modification.)

**Trust model / CMLA**

CMLA is a non-profit Limited Liability Corporation that has been founded by Intel, Matsushita, Nokia and Samsung to implement a trust model and PKI for systems based on the OMA DRM 2.0 technology. Recently CMLA has widened its scope to cover also mobile broadcast.

CMLA role can be seen as the insurance of the SPP system. CMLA is the third party that will neutrally analyze all problems. If misconduct has been identified, CMLA has the legal means to demand for improvements and in case all other efforts fail, use their legal power for terminal revocation and liability payments. This is clearly an improvement to the situation where one company would decide where the fault is and if liabilities are due.

CMLA as a trust model defines a widely accepted legal framework to ensure content security in download and broadcast services. At the time of the CMLA development all the major Hollywood studios and major record labels have been contributing in development of the model by setting the rules and expectations for the trust model.

Targets of the Mobile Broadcast related development within CMLA have been:

- Trust Model Uniformity – Trust model need to be uniform in a way that all the rules and requirement set for content security need to be present and unchanged regardless of the company or geographical region where the trust model is utilized.
- Security – Service and device implementations in content ecosystem defined by the trust model need to be implemented according highest applicable standards feasible in consumer electronics. Furthermore, trust model must be capable of enforcing all the ecosystem members to comply these implementation rules.
- Flexibility to business models – Trust model needs to be fully independent on business models and service models.
- Interoperability – Trust model need to ensure full interoperability of devices and services within the ecosystem.
- Low cost ecosystem – CMLA Trust Model need to provide industry best content and service protection at lowest cost possible to enable service providers to implement interesting and affordable service for end customers.

**CMLA:**

- Provides the necessary trust model, i.e. the legal framework defining
  - The level of robustness for all implementations
  - Appropriate penalties for vendors not being as robust as defined
- Issues keys and certificates for devices and rights issuers and run on-line parts of the PKI
- Enforce the CMLA Trust Model requirements if needed
- CMLA Trust Model includes the following agreements:
  - Client Adopter Agreement
  - Service Provider Agreement
  - Content Participant Agreement (This is optional for Content Owners)

More details can be found at [www.cm-la.com](http://www.cm-la.com).

# Executive summary

The Nseries Multimedia Computers offer various multimedia usage options for the user and service providers: pictures, video, music, Internet, interactive services and Mobile TV. Most of those services are pay-services requiring a mechanism to protect the content from misuse and to guarantee the rights owners their income from the content. Usually the content is DRM protected, but the later introduced broadcasted services need a new/enhanced system.

Use of Mobile TV media will grow fast and the business revenue potential is estimated to be high. The global subscriber base of Mobile TV users is estimated to reach 170 Million subscribers by 2010. The Mobile TV revenues are expected to be more than 14 billion USD by end of 2010. The sheer advertisement revenues of that being 1.1 Billion USD. (Source: iSuppli Corporation)

The Service Purchase and Protection system to be used with personal TV and Video must be bearer agnostic. The services may be consumed over a variety of channels (2G, 3G, DVB-H, DVB-T, WLAN) and having a system for each bearer would make service provider system setup extremely complicated. The use of a single solution independent of the delivery channel enables flexible use of system resources.

As DRM technologies are optimized for file handling, there has been a need to provide a further enhancement to the over mentioned technologies. Broadcasted or streamed services need those enhancements as they can not be treated as individual files. There are standardized technologies to support protection of any kind of content such as 18Crypt by ETSI and OMA BCAST specified DRM – and Smart Card Profiles.

Following the standards specified route has proven successful for Mobile industry. It has enabled a global market, interoperability, roaming and economies of scale. The adaptation of proprietary systems for spurious reasons would fragment the whole market and reduce its potential.

Major industry players worked together to design a global Service Purchase and Protection (SPP) system (18Crypt) to be used for broadcasted services. The group had members from all parties of a Mobile TV ecosystem: Broadcasters, Mobile Network operators, Component manufacturers, Security services company and terminal vendors.

The OMA organization has specified two systems to be used with Mobile Broadcasting. The OMA Smart Card Profile reuses elements of MBMS

security solution and is mandatory for terminals with mobile interaction channel. They have also adopted the 18Crypt system, and specified it further. The outcome, OMA DRM profile, is mandatory for terminals without a mobile interaction channel.

A standardized service and content protection solution provides the needed features. The OMA DRM profile (18Crypt) is versatile and not limited to only broadcast A/V but can be applied to any kind of IP based content. The DRM Profile (18Crypt) may be seen as a broadcast extension to Digital Rights Management (DRM) system. Secrets management of DRM profile (18Crypt) uses OMA DRM technology. OMA DRM 2.0 specified Rights Objects (RO) are used to deliver keys and entitlements. The terminal design follows the OMA design: Keys are stored and processed in a secure area inside a terminal. This enables the design of terminals which do not need SIM nor return channel (Pocket TV, Car TV) although the most common use for systems is expected to be in mobile handheld terminals with interaction channel.

The key benefits of a completely standardized Service and Content Protection system are:

- Compatibility with existing Mobile Ecosystem
- Interoperability between devices and network provides consumer friendly services
  - Roaming of services and terminals is possible
- Scale and growth advantage through a single solution
  - Global system guarantees a wide product offering with competitive pricing
- Suitability for any IP based content in mobile and fixed environments, not only streams and videos
- Scalability from DRM to broadcasted service protection with single system
- Time to markets and cost benefits through solutions that prevent market fragmentation
- Horizontal business models are possible
- Reuse of OMA DRM 2.0 technology for key delivery and distribution gives clear commercial and technical advantages (single system for DRM and SPP, single payments for technology IPR usage, simplicity of system overhead) over any competing system (OMA BCAST DRM profile)
- Use of OMA Smart Card Profile enables usage of single, bearer agnostic, Service Purchase and Protection system for all Mobile TV services
- Selecting the OMA BCAST standardized elements provides the optimum path to seamless offering of Mobile TV services
- Single vendor lock-in can be avoided

More information can be found at [www.nokia.com/mobiletv](http://www.nokia.com/mobiletv).

# Abbreviations & terms

**SP**, Service Protection. It is a method that ensures the service is received only by authorized recipient. The content itself may or may not be protected.

**SPP**, Service Purchase and Protection. Set of requirements defined by DVB for mobile TV service protection

**CP**, Content Protection. It is a method that limits the copying, reuse or redistribution of content to agreed audience.

**CA**, Conditional Access. The content may be of a nature (dedicated service, program,) that access to it needs to be limited just to the recipients that have bought the service.

**CMLA**, Content Management License Administrator. Is a licensing and compliance entity formed to provide a full solution implementation of the Open Mobile Alliance (OMA) Digital Rights Management (DRM) version 2.0 interoperability specification? [www.cm-la.com](http://www.cm-la.com)

**DRM**, Digital Rights Management. Technical methods used to control or restrict the use of digital media content on electronic devices with such technologies installed.

**Pay TV**, The requirement to protect the content after delivery comes through contractual obligations (license agreement for CA technology typically sets certain compliance and robustness rules). Legislation also makes selling circumvention devices illegal.

**FOTA**, Firmware Over The Air Update. A standardized mechanism to update terminal software over a mobile network.

**FTA**, Free To Air. The content is intended for everyone possessing a receiver.

**CTA**, Clear To Air. The content reception is free, but copying / forwarding not.

**18Crypt** Is an industry group that has developed a SP solution.

**OMA**, Open Mobile Alliance. A group defining standards for mobile industry.

**Subscription**. Is an operation mode of a Pay TV channel. The selected service is purchased for a period of time.

**PPV**, Pay Per view is an operation mode of a Pay TV channel. The selected service is purchased for immediate view. The content is time limited, usually a movie or similar.

© 2007 Nokia. All rights reserved. Nokia and Nokia Nseries are registered trademarks of Nokia Corporation. Other product or company names mentioned herein may be trademarks or registered trade names of respective owners.

Nokia Corporation  
PO Box 226  
FI-00045 Nokia Group  
Finland  
Phone: +358 (0) 7180 08000  
[www.nseries.com](http://www.nseries.com)  
[www.nokia.com/mobiletv](http://www.nokia.com/mobiletv)



**NOKIA**  
Nseries