

Service Protection within the Nokia IPDC Solution 2.2

Nokia IPDC Solution

The Nokia IPDC Solution implements Mobile TV service for DVB-H enabled handsets. A full end-to-end system for free-to-air TV requires only TV content, commercially available stream encoders and DVB-T transmitter equipment in addition to the Nokia IPDC Solution. For pay TV services the solution also needs to be integrated with the GSM service platform.

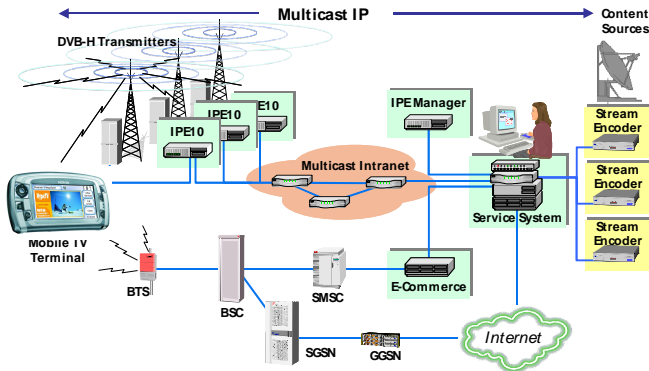


Figure 1: IPDC solution components marked against the end-to-end system

Service Protection Requirements



Figure 2: Subscribed and un-subscribed services listed in the Mobile TV terminal application user interface

Protection of services has been implemented in the Nokia IPDC Solution to prevent unauthorized consumption of paid content. The solution has been implemented to fulfill the following high-level requirements:

1. It shall be possible to flexibly bundle channels into packages, so that a particular service can be part of several packages and packages can contain several channels
2. Free-to-air, subscription-based and pay-per-view services shall be supported
3. Streams carrying paid content shall be encrypted with strong enough protection
4. Protection should be established with technologies already found in smart phones
5. Purchasing of paid content shall be seamlessly integrated to the Mobile TV application with immediate order fulfillment

Service Protection Architecture

Service protection is achieved with IPSec authentication and/or encryption with 56-bit DES algorithm. The *IPDC Service System* controls the encryption, which is carried out in the *IP Encapsulator* on a session-by-session basis. Each session is encrypted with its own key. Manual keying is used due to the unidirectional characteristics of the DVB-H network.

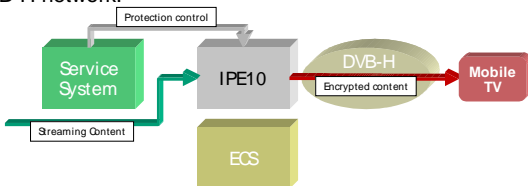


Figure 3: Content flow

The Service System also manages the service bundles, or *packages*. It generates an IPSec *security association file* for each package every day. The SA file for a given day details how each session can be decrypted by the terminal. The SA-file is *DRM*-encrypted, either with a

unique *rights object* (pay-per-view case) or with an RO changed monthly (subscription service). The encrypted SA-files are continuously broadcast to every DVB-H terminal using the ESG (Electronic Service Guide) time slice channel and the rights objects are sent daily to E-Commerce Systems.

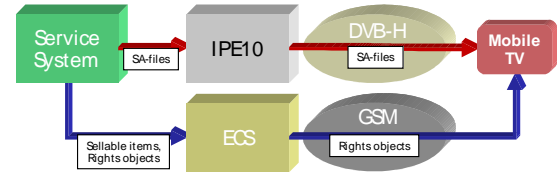


Figure 4: Key data flows

The end users can order viewing rights from the *IPDC E-Commerce System (ECS)*. ECS utilizes the unconfirmed WAP push protocol to deliver the rights objects to the DRM agent in the terminals. The agent prevents e.g. access to the IPSec keys and duplicating the RO or the SA-file. For continuous subscriptions, ECS pushes new rights objects to every subscriber's handset at the beginning of every calendar month until subscription is cancelled. ECS generates CDRs for billing purposes.

Level of Security

Current solution

The current Nokia IPDC Solution is intended for commercial pilots and the security level offered is more than sufficient for operation with a relatively small customer base. The system automatically generates both IPSec keys and DRM rights objects. Maximum life span for an IPSec security association is one day while DRM Rights Objects are valid for a month in the maximum.

Future direction

A more comprehensive solution is arguably required for commercial, mass-market deployment. The requirements will not change, but implementation will be made more secure. Together with the other industry players, Nokia is working within OMA to create a global standard for Mobile TV service protection as part of a standardized DVB-H terminal air interface. Details of the joint proposal can be found table below or in the OMA/DVB proposal.

Reference

Topic	Term	Description of IPDC implementation
IPDC Solution	SS	IPDC Service System: a server cluster, which controls all aspects of the Mobile TV service
	ECS	IPDC E-Commerce System: a server solution for DRM rights object delivery to end users
	CDR	Charging Detail Record: data record of a rights purchase; intended to be parsed by a billing system, which will invoice the end user for Mobile TV usage
	IPE	IPE10 IP Encapsulator: a IP-to-DVB gateway product
IPSec	AES	See DES
	HA	Header Authentication: protocol for remote party authentication and payload integrity verification
	ESP	Encapsulated Security Payload: protocol for payload traffic encryption
	DES	Data Encryption Standard: encryption algorithm, 56-bit variant is used currently in the IPSec encryption, while 128-bit AES is proposed as a basis for the standard solution
	SA	Security Association: data record consisting of source and target addresses, encryption algorithm and symmetrical secret key
Digital rights	OMA	Open Mobile Alliance: An industry forum

Service Protection within the Nokia IPDC Solution 2.2

management	DRM	Digital Rights Management: OMA standard for protection of digital content, version 1.0 used now and version 2.0 proposed as a basis for the standard solution
	forward lock	A mechanism, which prevents protected content from leaving the terminal.
	RO	Rights Object: data record consisting of usage rights related to an encrypted file
	separate delivery	A mechanism, where the protected content and usage rights are delivered via separate channels.