Smart Dongle

Feeling at home. Everywhere.

February 2007

BANKING & RETAIL

ENTREPRISE

INTERNET CONTENT PROVIDER

PUBLIC SECTOR & TRANSPORT

TELECOMMUNICATIONS>WHITE PAPER

gemalto
security to be free

Executive summary

TABLE OF CONTENTS

As the telecom ecosystem evolves, previously reliable revenue streams are being squeezed by traditional competition, regulatory pressure and new players. Customer behavior is also evolving, with ease of access to communication technology a priority for a population very much at home on the move.

Telecom operators are adapting their offers to meet customer demands, offering IP network coverage at home and in urban area, for example, and giving customers unlimited service access (voice and data) on any device and via any connection (Wireless, DSL, WiFi…).

This convergence of services, based on multiple channels and multiple devices, can be leveraged by the mobile operator. Gemalto has developed a dedicated convergent solution, spanning different form factors such as the smart USB Dongle and SIM/USIM, to give operators the following key capabilities:

- **strong authentication** - maintaining the link with subscriber (and ensuring billing!)
- **device personalization** - deploying and configuring the operator environment on any device
- **security** - protecting the link between customer and operator and guarding against phishing and spoofing, for example
- **connectivity** - enabling any communication application and generating new revenues

This paper describes one of the main elements of our convergence offer, the Smart Dongle. Plugged into a PC, Smart Dongle opens up all operator services and communicating applications to the subscriber. This new form factor allows the operator to enter the subscriber's PC environment to create promising services based on everyday customer devices.

.

Introduction

> Ecosystem evolution

Previously reliable revenue streams are being squeezed by traditional competition, regulatory pressure and new players. And customer behavior is also evolving - ease of access to communication technology is the priority for a population very much at home on the move.

Telecom operators are adapting their offers to meet customer demands - they're offering IP network coverage at home and in urban area, for example, and giving customers unlimited service access (voice and data) on any device and via any connection (Wireless, DSL, WiFi…).

As well as defining offers with price-appeal, in order to avoid churn to IP communication alternatives, the mobile operator need to:

• Consolidate the audience: delivering new services to maintain subscriber interest requires the operator to identify and understand the subscriber

• Address multiple devices to provide access to operator services from everyday subscriber devices

• Provide the subscriber with a safe environment, by setting up a secure and authenticated link for a trusting relationship between subscriber and services

• Deploy ready to use solutions - delivering plug-and-play without the barrier of complexity.

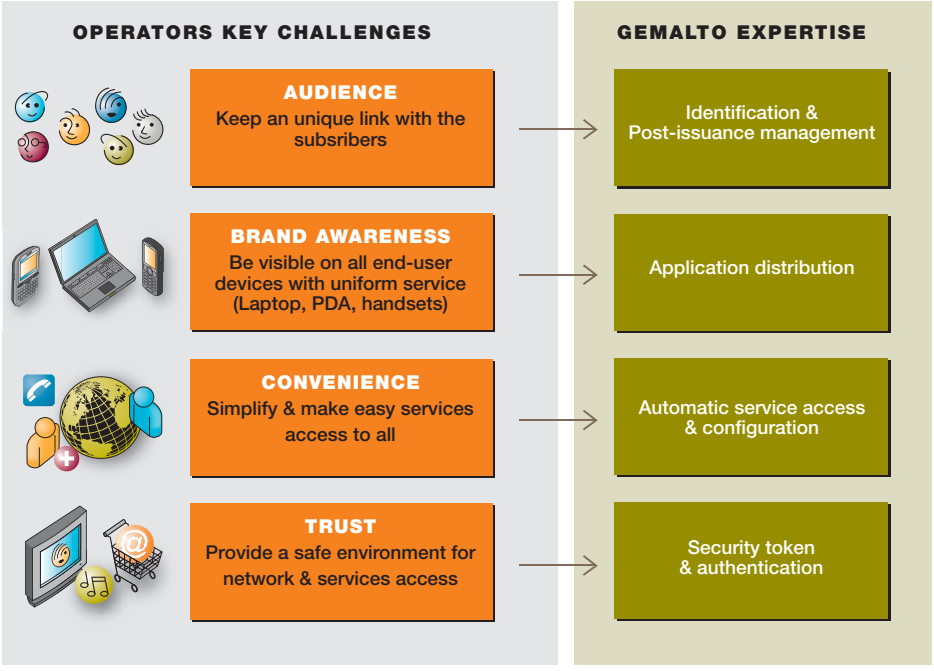
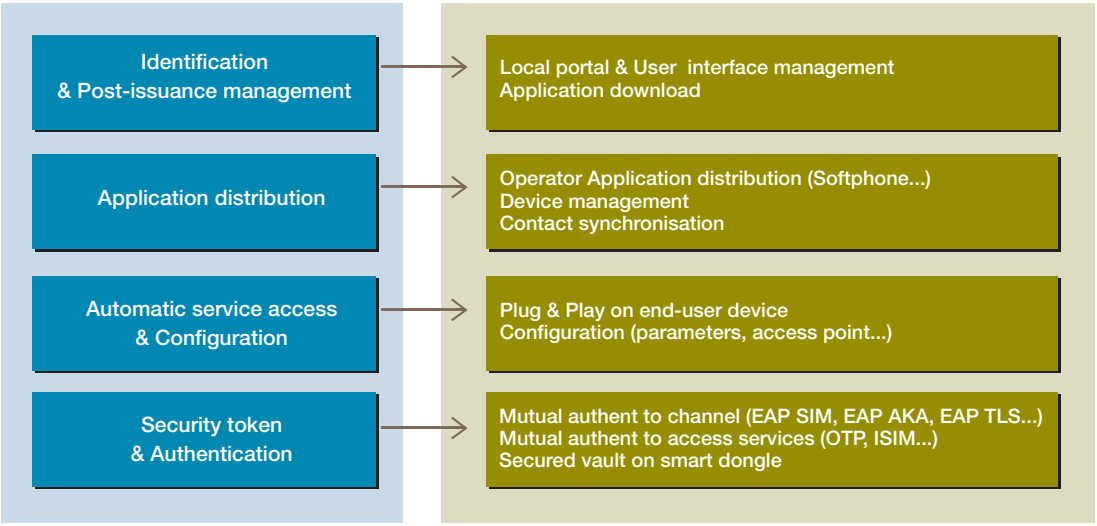


Fig1: Operator key challenges

The Gemalto Convergence offer is built on the key assets of the smart card: subscriber identification, data and channel security, device configuration and subscriber connectivity management.

Fig2: Smart card key assets



> Global Gemalto Convergence offer

Today's subscriber uses multiple devices, and requires the appropriate connectivity. To address this convergent ecosystem, Gemalto has defined a number of offers to match operator characteristics (pure mobile operator, mobile and ISP, and so on) and operator segmentation.

• **PC Link application**: By connecting a mobile phone to a PC with a local link (USB cable or WiFi for example) the subscriber automatically gains the benefits of an advanced personal data management solution, with local synchronization and on-line storage, and simple access to internet operator services with SIM -based authentication.

• **Smart Dongle**: By inserting Smart Dongle in a USB port on the PC, the subscriber gains access to operator IP services including voice and IM, and gains the benefits of the operator's proposals for attractive services using multimedia content and video, for example

• **Embedded smart card in PC**: The operator can easily build packaged offers for the corporate sector, including a PC with a complete and off-the–shelf connection manager.

• **Multi mode handset**: By using the SIM-based solution for managing GSM/3G service access and WiFi/WImax service access, the operator can come to the subscriber with a uniform trusted environment and combined offer.

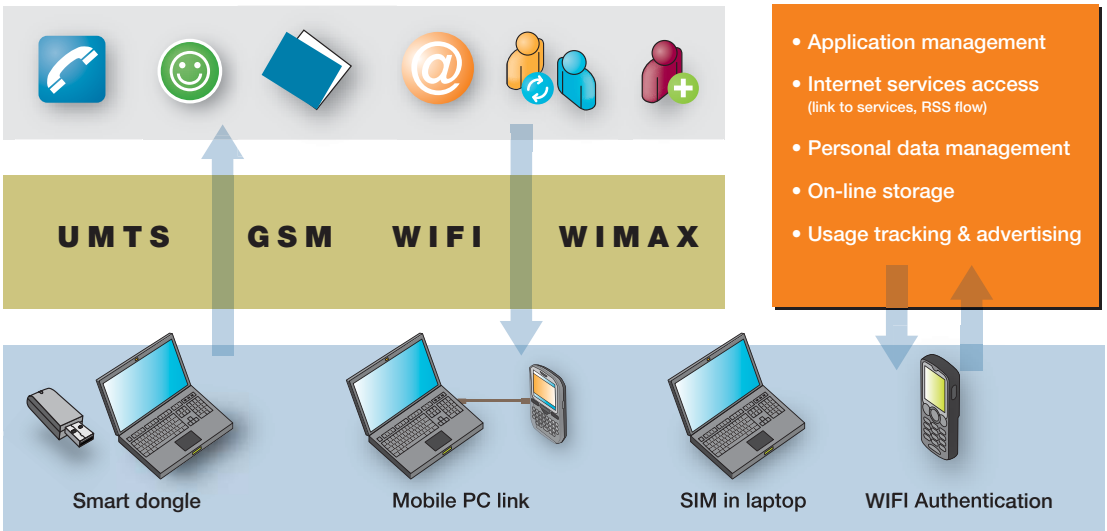


Fig3: Gemalto offer

As well as using these different form factors to address subscriber devices, Gemalto is enlarging its current OTA solution in order to provide the operator with an efficient way of managing the life cycle of the delivered application set. For each of these form factors, this over the internet (OTI) infrastructure offers the operator:

• **Application management:** Download, update, and delete applications offered

• **Internet service access:** Provide direct links to services, promote specific services depending on subscriber interests, offer information flow (RSS)

• **Personal data management:** Synchronize contact books for unification between all devices, back-up personal content and offer services for simple subscriber management of this content (picture printing for example)

• **On-line storage:** Provide unlimited storage space for the subscriber, automatically accessible when device connected

• **Usage tracking and advertising:** Analyze subscriber behavior, using this privileged link to consolidate audience and attract advertising capital

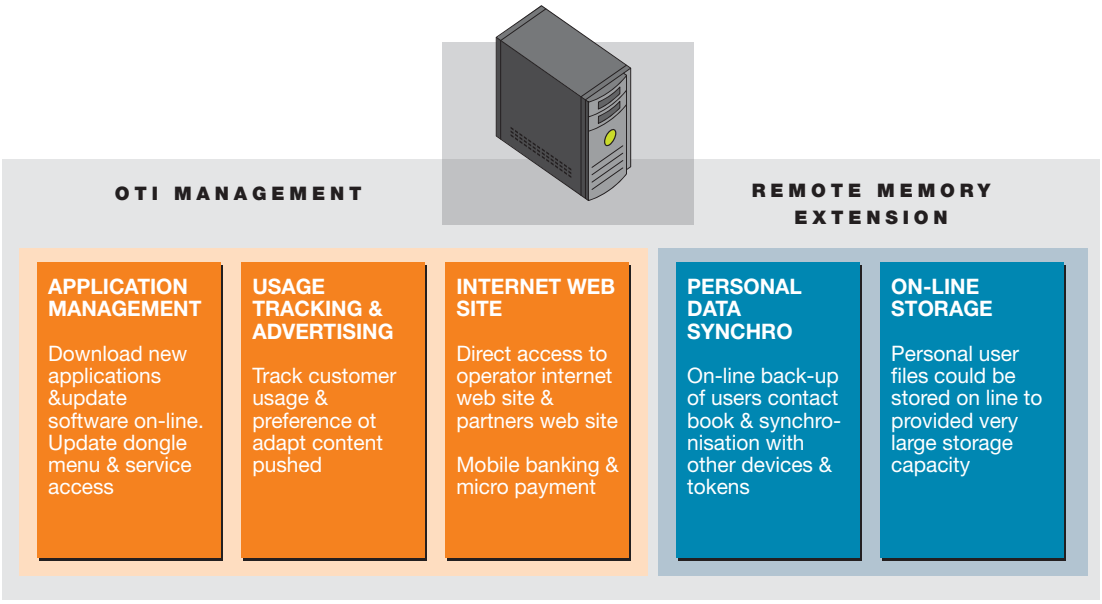


Fig4: Convergence offer management center

This paper focuses on the Smart Dongle offer. For additional information on the rest of the offer, specific white papers are available

> Smart Card dongle

Principles

Faced with increasing pressure from internet service providers entering the telecom world with services such as Instant Messaging or Voice Over IP, operators may consider deploying offers which allow end users to access their own internet services, whatever their location or the device they use. Subscriber behavior is also evolving. The laptop is now perceived as a powerful communication device, service access is not be limited to a specific area, and services are not be restricted to a single device.

Against that background, the Gemalto Smart Dongle solution can play a key role in:

• Reinforcing the link between the end-users through laptops and other connected devices

• Delivering service portability, to help prevent churn

• Implementing a convergence service offer on existing back-end infrastructure

• Consolidating the subscriber base while maintaining connectivity to the user regardless of device and access technology

Capabilities overview

Smart Dongle gives the operator the ability to provide service access via the end-user's laptop, with features such as auto configuration and automatic network access, and thus target devices that are outside the operator's scope today. It extends the operator's contact area with end users in their day to day communications.

Smart Dongle is extremely simple for any subscriber to use. After insertion in a USB port of the PC, a PIN pad is displayed on the screen for the subscriber to enter his secret code. After PIN verification, a menu is displayed on the screen offering the subscriber one-click access to his preferred services. These services can be stored on the dongle itself - Softphone, Media player, email and so on - or can be offered on-line - Multimedia content store, for example.

Any configuration of access channel or subscriber profile required is managed automatically by the dongle.

Linked to the application environment deployed through the dongle, memory (which may be protected or not) is offered for storing data linked with application, and any subscriber personal data.

With this complete kit, the subscriber can access preferred operator services from any PC. He or she can retrieve personal information (anywhere, anytime) and enjoy the benefits of the operator's attractive IP communications subscription.

Depending on the operator's strategy and coverage, this offer can be combined with a mobile subscription or an internet access subscription (DSL or WiFi).

Typical scenarios

In Business

Anthony works for the London office of a major audit company. He works hard, frequently very late at night, and he visits customers all around the world several times a year. He's good at his job, but he's not particularly organized. When traveling, Anthony likes to stay in touch with all his friends and colleagues sending his phone bill through the roof.
Thanks to the Smart Dongle, Anthony now has a fashionable token that resolves most of his issues:

- At work, he is receives all communications including voice and IM on the computer he's working on. He can also use the communication set to contact colleagues based everywhere in the world, at a very attractive price.
- When he gets home, he can finalize the PowerPoint presentation he stored on Smart Dongle on his personal computer, and start communicating with his friends to organize his next week end. Thanks to buddy list management, he only receives calls from his friends: all others are redirected to his voice mail.
- When traveling for business, he still benefits from the attractive communication subscription he gets with Smart Dongle and can spend time over the phone with his London office to prepare for a very important customer meeting.
- At night, he can access his own environment from any internet café, and start exchanging content, navigating preferred internet services and communicating with friends using the same environment.

Within the Family:

Before giving his sons John and William their own Smart Dongle, Daniel Ingalls was facing several problems: his fixed line was always tied up by never-ending conversation between one of his sons and his Spanish girl friend, the monthly phone bill was breaking new records at the end of every month, and his sons were taking their brand-new laptops around from one friend's home to another, with a high risk of damage.
Now, with their own Smart Dongle combined with a mobile subscription:

- Daniel sponsors three hours' VoIP for his sons
- Instead of using the home phone, John and William use the Softphone on their laptops in their room. All communications are attractively priced, and are consolidated in their mobile subscription.
- When going round to a friend's house, John and William just take their smart dongle with all the data and applications they want to share.
- When they are traveling, John and William can now call their parents as often as they like, without risking running out of money
- When John is traveling, he can easily post his latest photos on his on-line storage area, to share with family and friends. On the photo back-up area, he can also arrange for the best ones to be printed,

> Smart Dongle Use cases

Plug & Play

Once inserted in the USB port of the subscriber computer, Smart Dongle's auto-run capability triggers the processes managing connection parameters to the operator network. The PIN pad for subscriber authentication is automatically displayed, and after PIN verification the launch pad presenting all applications or memory resources on the Dongle is automatically displayed on the computer screen.

By just entering his PIN code, the subscriber has his application environment operational (in term of application availability, channel availability, channel authentication).
The list of actions triggered during this initialization process is adapted to the individual operator's strategy - channel access (WiFi, DSL) can be handled automatically during initialization or triggered by the subscriber when connection is needed, for example.

The Smart Dongle works on any computer without any library installation.

Identification

Network access

If needed and after the initial auto-installation session, the client on the PC triggers an automatic authentication to the network. Different methods of network authentication to WiFi or DSL could be proposed: EAP-SIM and EAP-AKA. Both have been standardized by IETF, IEEE, ETSI and 3GPP.

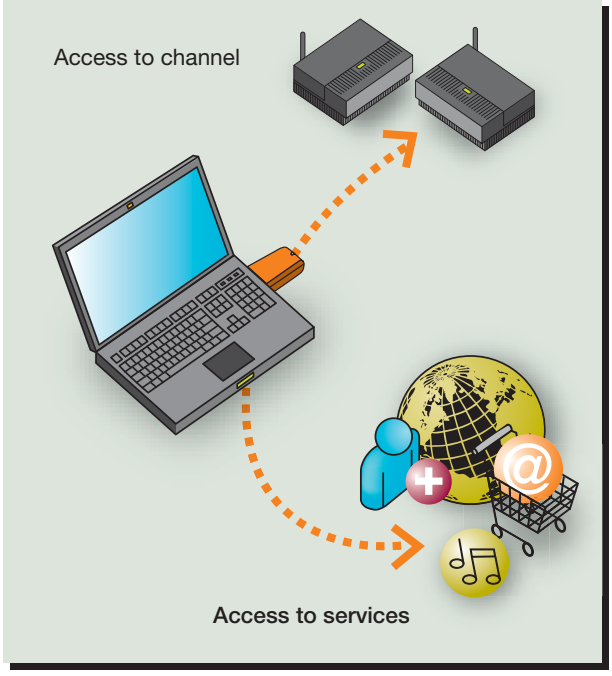
Users can access the operator's network anywhere: at home, through hot spots when traveling, at the office…

Services access

Independent of network authentication, Smart Dongle also supports automatic connection to services. Users can manage their own preferences, avoiding the need to remember login/passwords on different web sites. The user, after launching his browser (that can be part of portable application stored on the dongle), will retrieve all personal bookmarks. The login details for each of these are stored in the dongle. Smart Dongle performs the security details transfer and connects to service.

Additionally, for services provided on top of WiFi or DSL, the smart dongle enhances the security of the authentication methods:

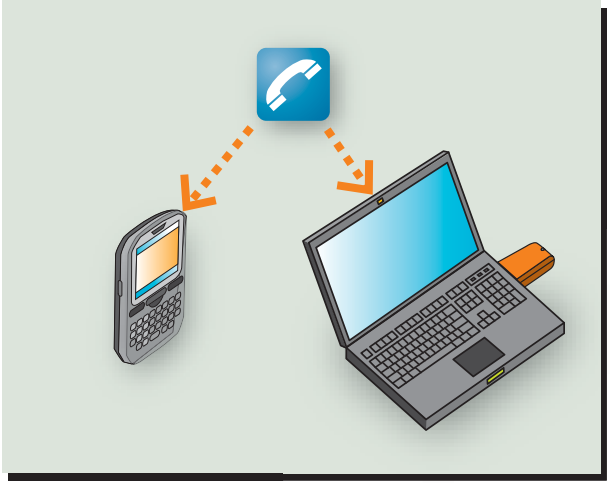
- ISIM (IMS SIM) to allow access to IMS services
- VPN (Virtual Private Network) to access corporate networks
- GBA-U Generic Bootstrap architecture with USIM
- OTP (One-Time Password) to access web services
- CAS (Conditional Access System) for digital TV



Presence management

When inserting Smart Dongle in the computer, all communication can be redirected to the computer in the case of UMA or SIP architecture, or the subscriber can define the rules to be applied for communication in the case of SIP architecture - all calls redirected to the computer, calls received on computer and handset, and so on.

On top of communication re-routing, content received can also be adapted to the device used. In the case of presence notification on the computer, the user interface for instant messaging applications can be much richer, compared to the same application accessed from a handset.



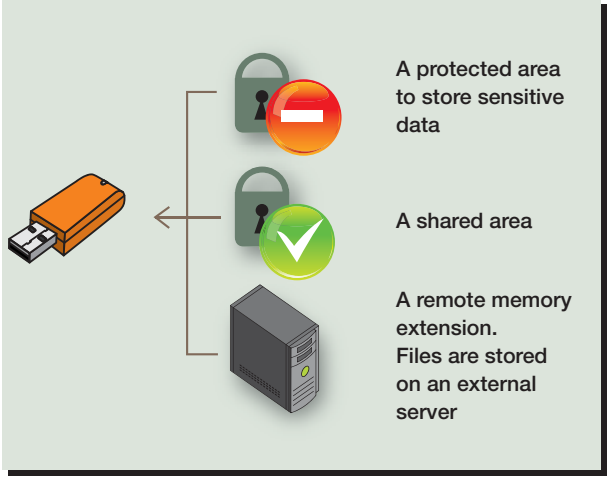
Memory & Privacy

Smart Dongle also incorporates embedded mass storage. This area can be split into several parts, with different memory spaces. One of these areas could be allocated to the operator for tasks such as remote administration of Smart Dongle, updating embedded services, and data synchronization, and the remaining memory split into a personal area for confidential data storage, and a shared area.

If protected, the personal area would only be accessed by the end user, after supplying a PIN code, and used for confidential files, but also login/passwords information, the phone book, DRMs on music and videos, and so on. The shared area could be accessed by anyone, as for a standard USB key.

On top of the local memory storage, after PIN verification automatic server authentication can be performed to open a personal on-line space. This space can be used for data back-up, for example, or data exchange with authorized contacts. In this on-line storage, the operator can offer the subscriber various services for managing his personal content, such as video tools and photo printing.

To reflect the operator's strategy, Gemalto can offer embedded Smart Dongle memory to support only operator applications and data (~512MB) or a complete solution embedding operator memory and subscriber memory.



Application platform

Smart Dongle incorporates an embedded set of application that can be easily used by the subscriber on any computer. Different types of applications can be hosted on the dongle:

• **Communication applications**, like VoIP phone or IM tools. These applications give the subscriber all tools needed to communicate with friends or colleagues. These applications are provided by the operator and integrated in its communication infrastructure. For VoIP, depending on the operator's existing architecture, it can be based on SIP technology or UMA technology. A mobile operator may choose UMA technology for managing the Softphone in the same way any mobile phones are managed. For operators wishing to integrate these communication tools in IMS-like architecture, SIP technology will be used.

• **Computer Office applications**, like internet browsers and email. These applications allow the subscriber to retrieve his own environment (favorites, bookmarks, emails…) on any computer, regardless of the application set already installed on this computer.

• **Entertainment application** such as a media player or video creation manager. These applications ensure that the subscriber always has the right application available to manage personal content stored on Smart Dongle or in the on-line storage area.

All these application are provided on Smart Dongle in portable-apps format, to reflect the nomadic lifestyle of today's subscribers.

Nomadic lifestyle

Using Smart Dongle, users can access their entire personal environment on all connected devices. This “mobile PC” concept supports a completely nomadic lifestyle. The USB drive business is also moving from pure data storage, to data with related applications storage.

Portability of operator environment

Smart Dongle triggers applications and icons provided by the operator
- It indicates that the user is logged to operator network
- User can click to launch additional Smart Dongle functions – all operator-branded

Portability of end-user environment

The “portable apps” feature enables the user to access his or her applications on any machine. There is no longer any need to use 'my' PC, because all the applications are embedded in Smart Dongle - browser, VoIP agent, work applications and so on.
The end user can thus:
- work at a customer's premises
- work at home on the 'leisure' PC, even if it does not support the same applications set

The user inserts Smart Dongle, selects the application and launches it in a simple click, directly from the dongle. When the user closes the application and removes the dongle, no fingerprint is left on the guest PC. So a user can work at customer premises, for example, without any threat to confidentiality.

Portability of datas

As on any USB key, the user can store all data on the memory space offered by Smart Dongle, up to gigabytes.

Safe environment

Smart Dongle can be inserted on any computer, can be accessed from the Smart Dongle management center, and offers internet access to the subscriber - in other words, it's out there in an IP open environment with all its risks for the subscriber: phishing, dongle spy ware attacks, and so on.

So to provide the subscriber with a safe environment, Smart Dongle embeds the following security schemes:

• **Mutual authentication** between subscriber and operator for ensuring that the subscriber exchanges information with the right service provider (mechanisms like EAP SIM/AKA and EAP TLS are supported)

• **Channel securization** for protecting data to be exchanged (data ciphering).

• **Secured channel between the host (PC, laptop) and the Smart Dongle** so only certified applications are allowed access to Smart Dongle capabilities. This secured channel is mandatory to prevent any spyware installed on the PC attacking the dongle.

• **Secured channel between Smart Dongle management center and Smart Dongle** itself for avoiding any non-certified server accessing smart dongle capabilities.

These mechanisms are transparent for the subscriber. This safe environment based on smart card technology will foster a strong preference on the part of the subscriber for using new services proposed by the operator, and for using that operator's services rather than those from another provider.

Life Cycle management

On top of Smart Dongle and all associated industrialization and personalization processes, Gemalto is building a complete server infrastructure for managing the life cycle of the dongle and providing subscribers with the help they need to get the most from their dongles. The OTI-based server focuses on five main areas:

• **Application management**: Download, update, and delete applications offered on Smart Dongle - for example, a Softphone update or the download of a new media player application.

• **Internet service access**: Provide direct links to services, promote specific services depending on subscriber interests, offer information flow (RSS)

• **Personal data management**: Synchronize contact books for unification between all devices, back-up personal content and offer services for simple subscriber content management, such as photo printing

• **On-line storage**: Provide unlimited storage space, automatically accessed when the device is connected

• **Usage tracking and advertising**: Analyze subscriber behavior, using this privileged link to consolidate the audience and attract advertising capital

> Gemalto offer key benefits

Smart Dongle is part of a complete solution and process including industrialization and personalization, Smart Dongle management center server, and applications for life cycle management. The Gemalto solution provides the operator with the following key success factors:

• An advanced Smart Dongle architecture to enable a secure link between PC and dongle and server and dongle

• An established personalization process, integrated within the operator infrastructure to optimize offer go-to-market

• Eight years experience in secured token life cycle management (317 solutions deployed, 665M subscribers) for a robust, future proof and reliable dongle management center

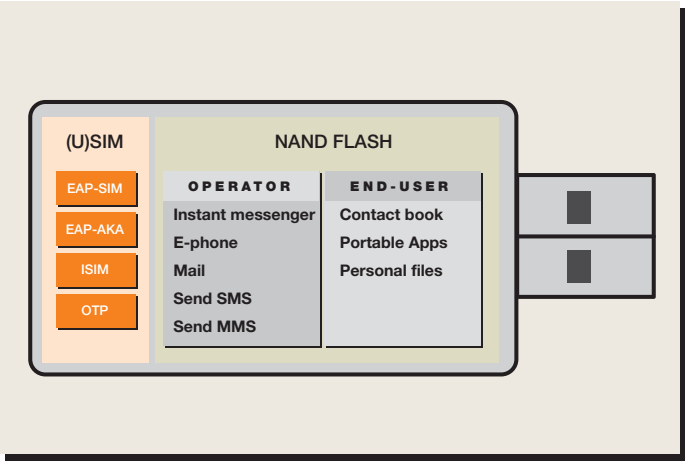
• A integrated solution including hardware, deployment, server and applications for simpler deployment management and time to market efficiency.

• Best in class security, already acknowledged in the banking, ID and Telecom markets, to provide subscribers with a safe environment that will encourage them to use the operator more frequently

• Access to highly experienced teams with the skills to customize solutions for specific infrastructures and markets, backed by the most substantial R&D resource in the industry.

> Architecture

As the use cases show, Smart Dongle is autonomous and just needs a host to deploy the operator environment automatically and allow the user to access the operator's services.

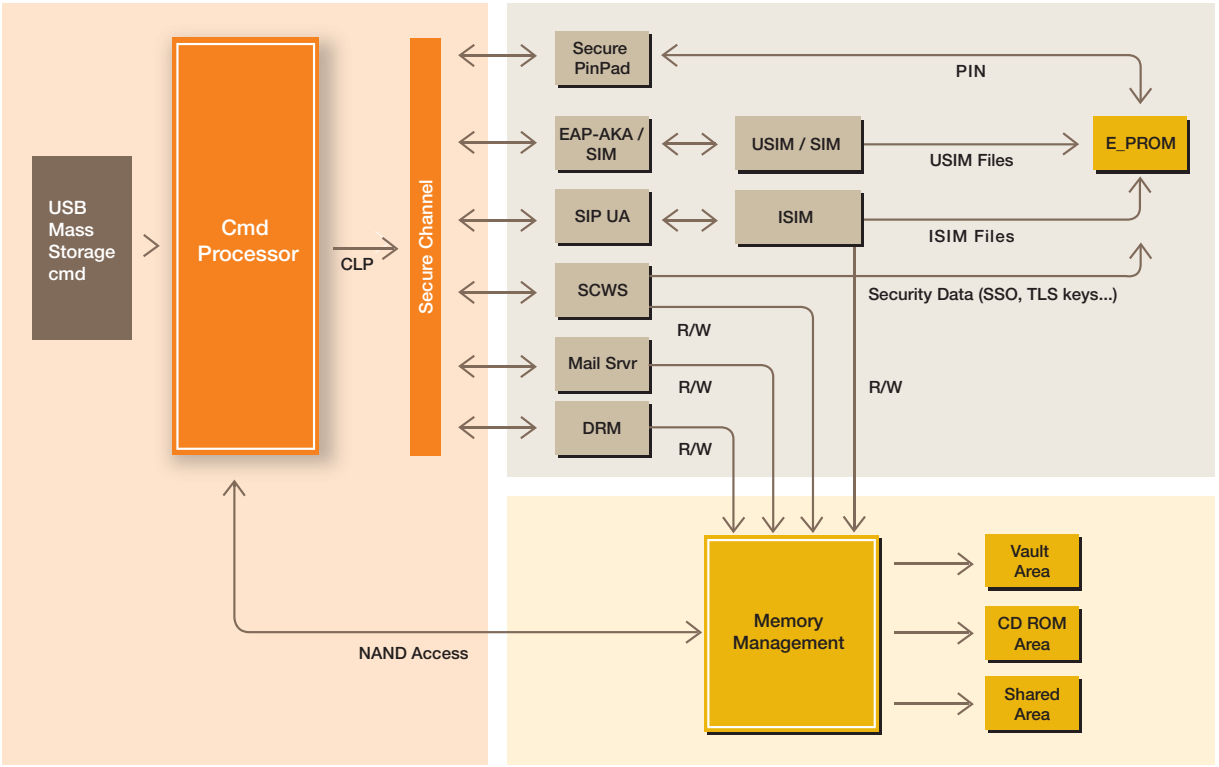


There are two different cases of Smart Dongle usage:

1 - inserted in the owner's PC. All the applications and driver required can be installed on the computer to provide the best environment. In this case, the Smart Dongle is only used to easily deploy the operator environment and related configuration on the subscriber's PC.

2 - inserted in any PC. In this case the Smart Dongle will not pollute the host PC with drivers or file installations. When Smart Dongle is extracted from the host, nothing remains on the PC.

The figure below presents the high level Smart Dongle architecture, taking into account the fact that the dongle needs to be transportable (nomadic) making the need to represent the user on the network (SIP user agent + SIP card agent).



Annex : Key concepts detailed description

> Portable environment and autorun

These two concepts are used to deploy the end-user environment at each Smart Dongle insertion.
The autorun allows a specific application to be run giving access to all Smart Dongle functions (storage, secure storage, Operator Connection manager, Operator service manager, contact book, and portable applications). This application can be considered as a portable environment dashboard. This dashboard quickly pops up on the user PC screen at dongle insertion.
A portable application is a PC application installed on removable media (i.e.: a dongle) and run in the host system memory without installing anything on the host platform. No settings will be added to the registry, no data will remain on the host disk, no footprint will be retrieved on the PC.
As an example, a mail client can be installed in the dongle with the user account personal configuration and can be launched by the user each time the dongle is inserted.

> Authentication: EAP-SIM/AKA

Both EAP-SIM and EAP-AKA are used to authenticate a subscriber to an access network.
The difference between those two methods is that EAP-SIM relies on SIM algorithms used in 2G networks and EAP-AKA relies on AKA used in 3G networks. SIM perform a unilateral authentication where AKA perform a mutual authentication. The EAP-SIM adds the network authentication missing in the 2G scheme, making these two methods equal in term of level of security (used algorithm not include in this analysis).

These two methods are designed to authenticate a token via the existing operator infrastructure. It relies on the usage of the SIM or UICC. It brings strong authentication (Mutual authentication), and generates keying material and stronger ciphering keys

EAP SIM is defined in the RFC 4186, (January 2006), coming from 3GPP. This is the EAP for GSM Subscriber Identity.
An enhancement to GSM authentication and key agreement is the possibility of combining multiple authentication triplets to create authentication responses and session keys of greater strength than the individual GSM triplets.

EAP AKA is defined in the RFC 4187, January 2006, coming from 3GPP. This is the EAP for USIM, R-UIM.

- This EAP mechanism uses the Authentication and Key Agreement (AKA) mechanism.
- AKA is based on symmetric keys, and runs in a UMTS Subscriber Identity Module, USIM, or a (Removable) User Identity Module, (R)UIM, similar to a smart card.

It has been defined to support WLAN interworking with UMTS

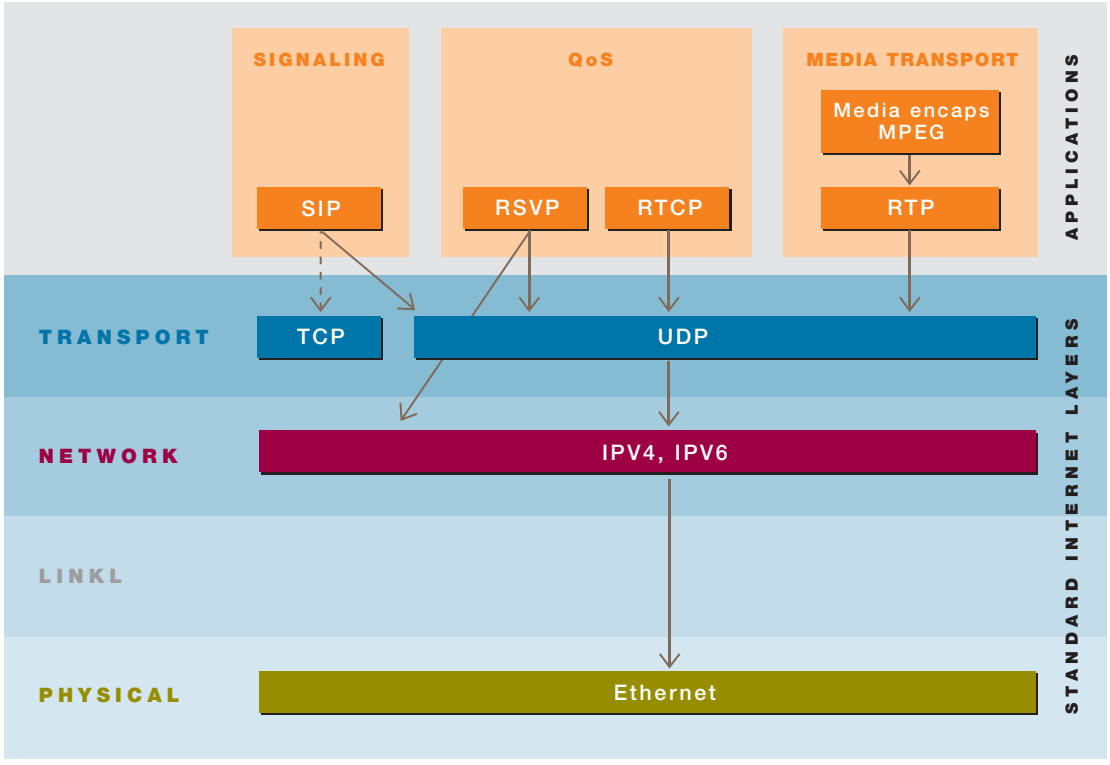
> Presence and Call Processing

Presence management is the way an end user will manage the visibility other connected persons will have of him or her.
Call processing is the way in which the user will manage incoming calls on different connected and registered devices.
These two services are linked to user contacts list (as presence and call processing can be set differently for a group of contacts to another) and are managed through the SIP protocol and some specific web services (XML over HTTP).
We shall consider that the user will be present on the network over different devices and different access networks and will wish to set specific rules depending on current activity and availability. These rules shall be applied on all connected devices and a live synchronization will have to be processed.
These rules need to be part of the user's Contact database, preferably stored in the removable Smart Dongle to allow secured OTI/OTA management (backup) and device agnosticism.
Smart Dongle can simply assure the storage of these rules or be part of a distributed application where rules are enforced in the card.

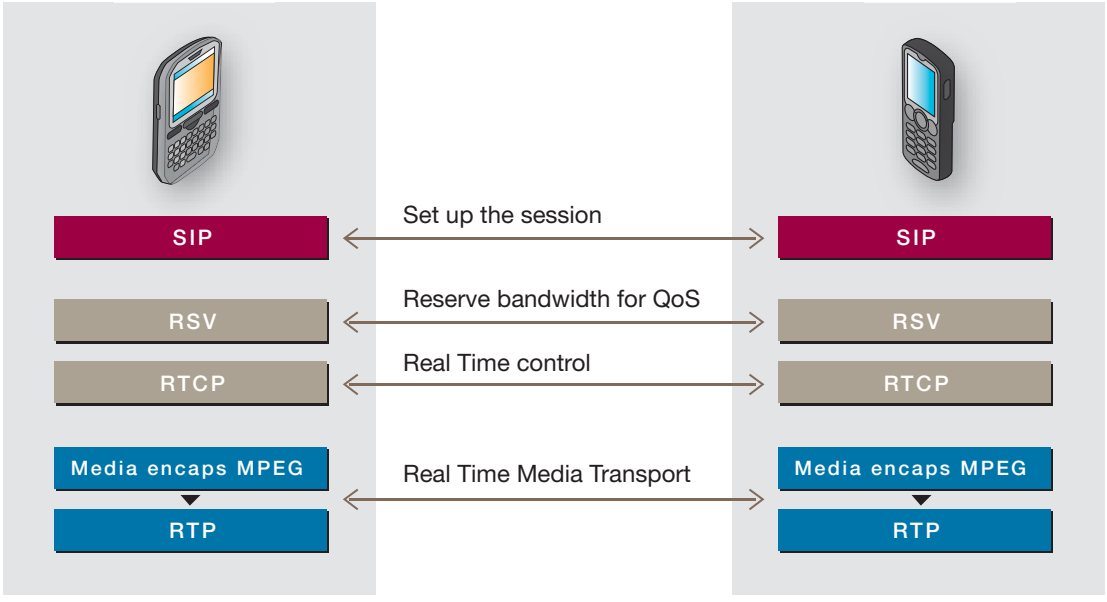
> SIP User agent

The SIP user agent is the part of a Communicator User Agent (with VoIP, IM, and more) which handles the SIP protocol to establish communications.
The idea is to let the card manage all SIP operations for the hosting device internally. This means the authentication part of the SIP registration process will be transparent to the hosting device, closing the door to some possible attacks.
The other interest of this separated implementation is to deliver directly the rules (call processing) to the networks, or enforce them internally in the UA. A modification on these rules can be pushed to other SIP UA if needed.

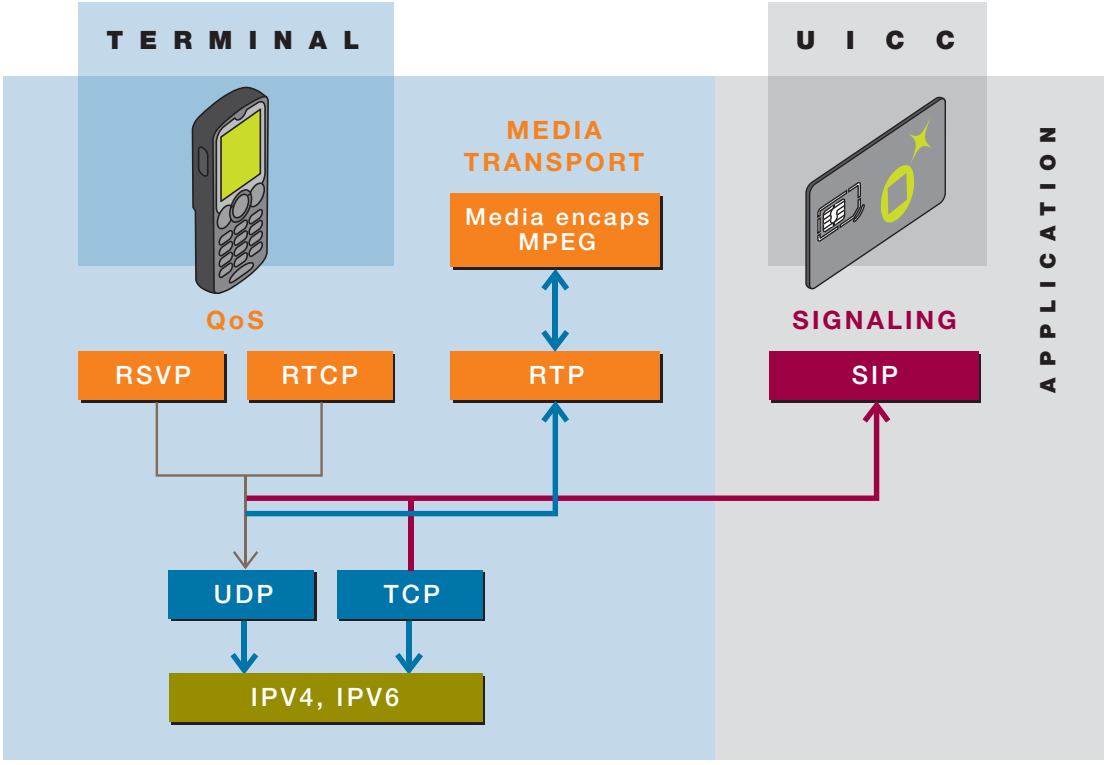
The following picture gives an overview of different protocols that are present in a VoIP (or other communications agent) user agent with the three different functions: signaling to setup the media session, the QoS to assure the needed bandwidth and the media itself transporting the codec of the voice.



The following picture shows how two devices are connected using each of the protocols described above.



The following picture provides an example of how a user agent can be implemented using the card. All Signalling operations are provided by the card when all other protocols are kept on the host. The main reasons for such a split are that the signaling is linked to user and is used for the user authentication, and that rules managing incoming calls are set by the user , stored and applied in the card. As the card already stores all user data, and is already used for user authentication there's good reasons for keeping everything linked to the user in the card, to avoid privacy and security issues.



> IMS

IMS means Internet Multimedia "Sub"-system but should be considered as the "core" network as it is the way to deliver services to the end user (the Principal) with complete independence from the access network.
IMS relies on three core and major features:
- The IP protocol availability.
- The capability to be always on. The access network needs to provide always on connectivity, even if is something that is not so easy for the mobile network infrastructure.
-The SIP protocol (Session initiation protocol) brings the signaling on IP network, meaning that all multimedia sessions will be set up through SIP exchanges.

The IMS core network shall be able to address legacy services and new services.
Telephony is an example of a legacy service that will help IMS adoption, but Video Sharing, presence management, or call processing are good examples of new services that will tease the user to adopt IMS based services.

Even if all these services are already possible in 3G or Fixed DSL network, IMS will boost their deployment and usage, by making them available from any device, on any network and at any time. Coming on top of the multiple existing infrastructures, IMS will thus achieve full integration of services, giving full ubiquity and connectivity to the users.

The SIP protocol is used to register to the IMS network, and this registering requires user authentication. It is possible to use many different authentication algorithms in SIP register authentication, but using a smart card brings four major advantages:
• Strong authentication (up to date and strong cryptographic algorithms and keys)
• Ease authentication secrets distribution
• The ISIM application comes with all service and subscription information needed to deliver services
• Allows roaming and device replacement with no need of remote provisioning operations.

Glossary

SMART CARD : In this paper a smart card can take more than ISO 7816 card format, and embed a secure silicon that will ensure the processing of functions such as cryptographic computation, device management operation (protocols) or SIP and HTTP support.

AKA : Authentication Key agrement protocol defined by 3GPP used in 3G mobile networks. This is the mechanism by which the User Equipement is authentified in a 3G network.

UICC : The Smart Card platform able to support USIM, ISIM and other smart card applicaions.

SIM : Subscriber Identity module used in GSM networks.

USIM : Universal Subscriber Identity module used in UMTS networks.

ISIM : IMS Subcsriber Identity module

SIP UA : Session Initiation protocl User Agent

OTI : Over the Internet. This acronym comes from OTA (Over the Air) which is the remote card management mechanism used in mobile telephony (GSM, UMTS). With new networks, the need is to address the card using IP protocols. This is what is done with OTI mechanism that can apply to any smart card described in this document.

ETSI : European Telecommunications Institute, where are defined and produced most of standards used to define USIM, ISIM and SIM.

IEEE : Institute of Electrical and Electronics Engineers, in charge of Wifi and Wimax.

3GPP : Third generation partnership project, in charge of defining services and network architecures for mobile telecommunications.

3GPP2 : Third generation partnership project 2, in charge of defining a services and network architectures for mobile telecommunications. This forum re-use most of 3GPP specifications and is mostly used in North America.

AuC Authentication center : Authentication server used in 3G and 2G networks. This is the part in charge to generate the Authentication vector used to authenticate the User equipment through the USIM (or SIM). Using the EAP-SIM, EAP-AKA, ISIM, GBA, allows to re-use this server to generate authentication vectors that will be used at different layers of the service (Access network, IMS network, and service itself).
Using this same server, help the operator to ease the subscriber billing as all access are managed through the same equipment.

HSS Home Subscriber Server : This is the subscriber database that is used in IMS networks. This HSS is very close to an HLR/AuC equipement.

A wide range of solutions

www.gemalto.com

gemalto
security to be free