

Fixed Mobile Convergence

Dr. Stephan Spitz

Giesecke & Devrient GmbH
Division Telecommunication



Fixed Mobile Convergence (FMC)

- 1. What is FMC ? Technology Status of FMC**
- 2. Existing (U/I)SIM-based FMC security solutions**
- 3. The Future**



Fixed Mobile Convergence (FMC)

- 1. What is FMC ? Technology Status of FMC**
2. Existing (U/I)SIM-based FMC security solutions
3. The Future

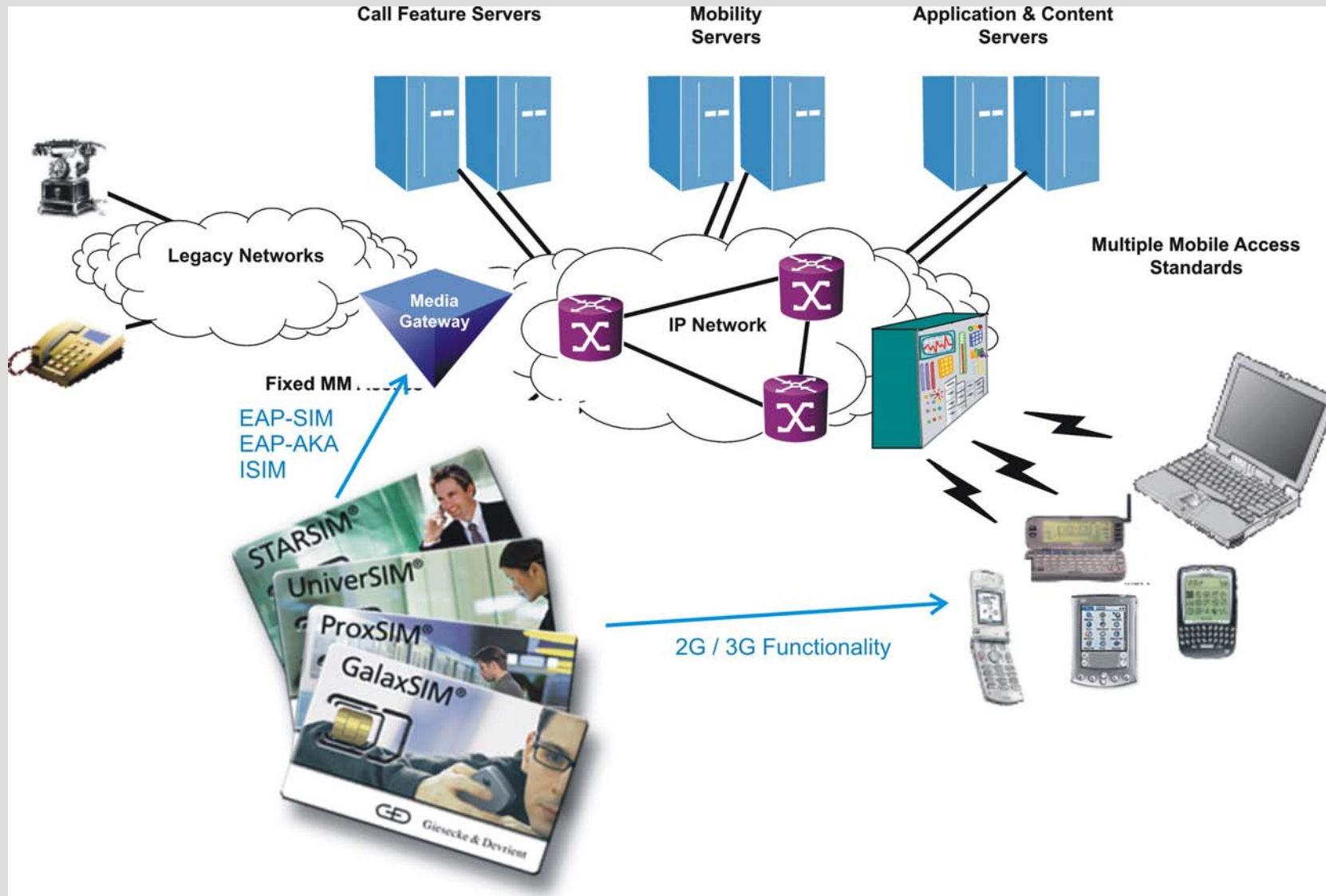


Definition of Fixed Mobile Convergence, ...

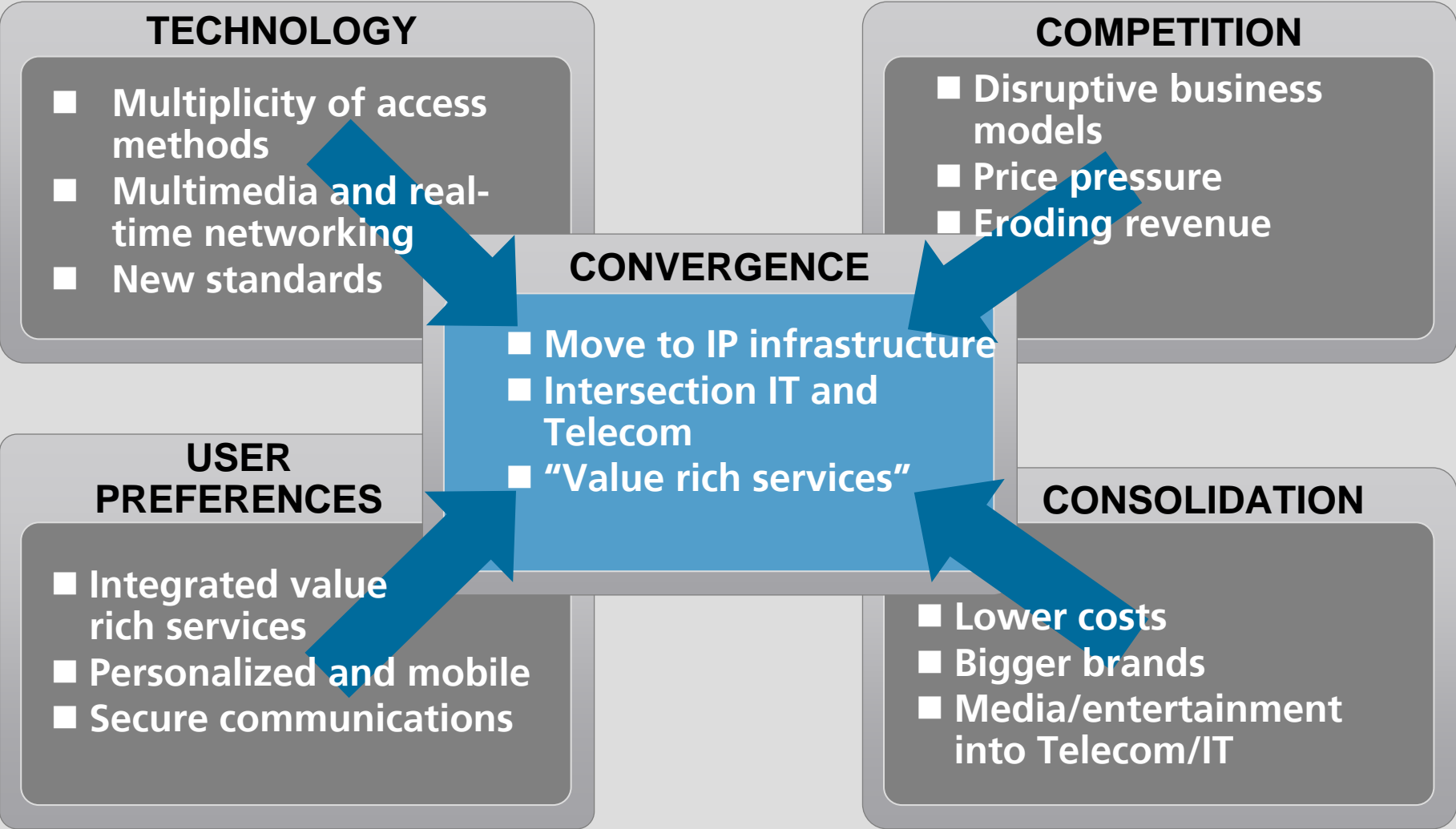
The aim of Fixed Mobile Convergence (FMC) is to provide fixed and mobile services with a single phone or personal device, which could switch between networks ad hoc.

Wikipedia

... but also Network Convergence



Strong Convergence Drivers



Standardization Bodies

- **TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks) specifications of 3GPP ensure integration between fixed and mobile solutions based on 3GPP IMS (IP Multimedia Subsystem)**
<http://www.etsi.org/tispan/>; WG7 SEC security
- **Fixed Mobile Convergence Alliance (FMCA,**
<http://www.thefmca.com>)
- **WiMAX Forum (<http://www.wimaxforum.org>)**

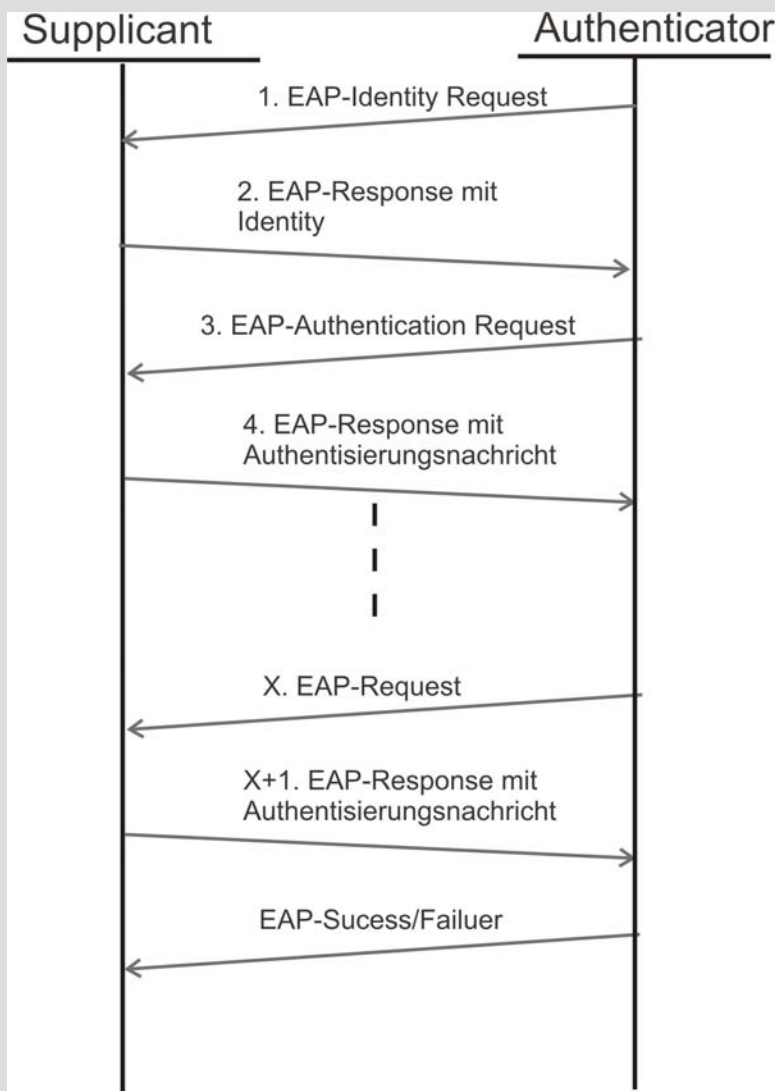
Some FMC Examples

- TwinTel (<http://www.arcor.de/privat/twintel.jsp>) in Germany: Arcor offers a mobile GSM handset which can also be used for making calls through the ADSL line
- BT Fusion* (<http://www.btfusionorder.bt.com/>) in England: British Telecom offers a Vodafone handset also capable of making calls through the ADSL line.
- Beautiful Phone (<http://www.beautifulphone.com/html/en/>) in France: neuf cegetel offers also a combined fixed mobile phone.
- Free a french Internet provider (<http://adsl.free.fr/>), develops a WiFi mesh network of HD „freeboxes“ to be used to provide mobile telephony
- unik: Orange offers a single telephone, a single number, a single address book, at home or on the move www.unik.orange.fr

Fixed Mobile Convergence (FMC)

1. What is FMC ? Technology Status of FMC
2. Existing (U/I)SIM-based FMC security solutions
3. The Future

EAP in general



- **“Only” authentication to the WLAN access point (no end-to-end security)**
- **EAP is specified in RFC 3748**
- **A lot of EAP authentication mechanisms are available (40) e.g. EAP-MD5, EAP-TLS,...**
- **(U)SIM relevant are**
 - **EAP-SIM based on 2G authentication**
 - **EAP-AKA based on 3G authentication**

EAP-SIM

- RFC 4186 specifies an authentication mechanism in which a SIM's encryption key used in GSM systems is applied for EAP authentication
- For security reasons triplets are used, because GSM key length is considered as too short
- Both sides (supplicant and authenticator) have to share the same symmetric (GSM authentication) key for the authentication process
- Different implementation variants on the SIM are possible depending on the communication between ME and SIM

EAP-AKA

- RFC 4187 specifies an EAP authentication mechanism based on an USIM and the UMTS AKA (Authentication and Key Agreement) protocol
- The authentication vector used with AKA is applied for this special EAP authentication
- With the UMTS authentication also the provider/authenticator is authenticated by the handset/supplicant
- Both sides (supplicant and authenticator) have to share the same symmetric (UMTS authentication) key for the authentication process
- No technical challenge for the USIM card itself, but again different implementation variants on the USIM are possible depending on the communication between ME and SIM

ISIM (IP Multimedia Subsystem) SIM 1/2

- **The IMS (IP Multimedia Subsystem) specified by the 3GPP TISPAN offers among other services Push-To-Talk, VoIP, Video and Content Sharing, Instant Messaging and Unified Messaging**
- **ISIM Functionality: Authentication to the operator or carrier supporting an IMS service via the Generic Bootstrapping Architecture (GBA)**
- **USIM and ISIM security algorithm are the same with IMS AKA i.e. authentication based on pre-shared symmetric keys**
- **The AKA authentication vector again is applied for IMS AKA authentication (like EAP-AKA)**

ISIM (IP Multimedia Subsystem) SIM 2/2

- **Confidential Data stored on ISIM: user's subscription level, keys i.e. authentication and security information and the private identity of the subscriber**
- **The private identity is linked to a public identity e.g. a SIP URI "user@mynet" or TEL URI "+49-89-4119-0@mynet". Moreover an IMS private identity can be resolved from the user's IMSI**
- **ISIM and USIM functionality can be easily combined on one module**

Fixed Mobile Convergence (FMC)

1. What is FMC ? Technology Status of FMC
2. Existing (U/I)SIM-based FMC security solutions
3. The Future

The Future: FMC and G&D's GalaxSIM

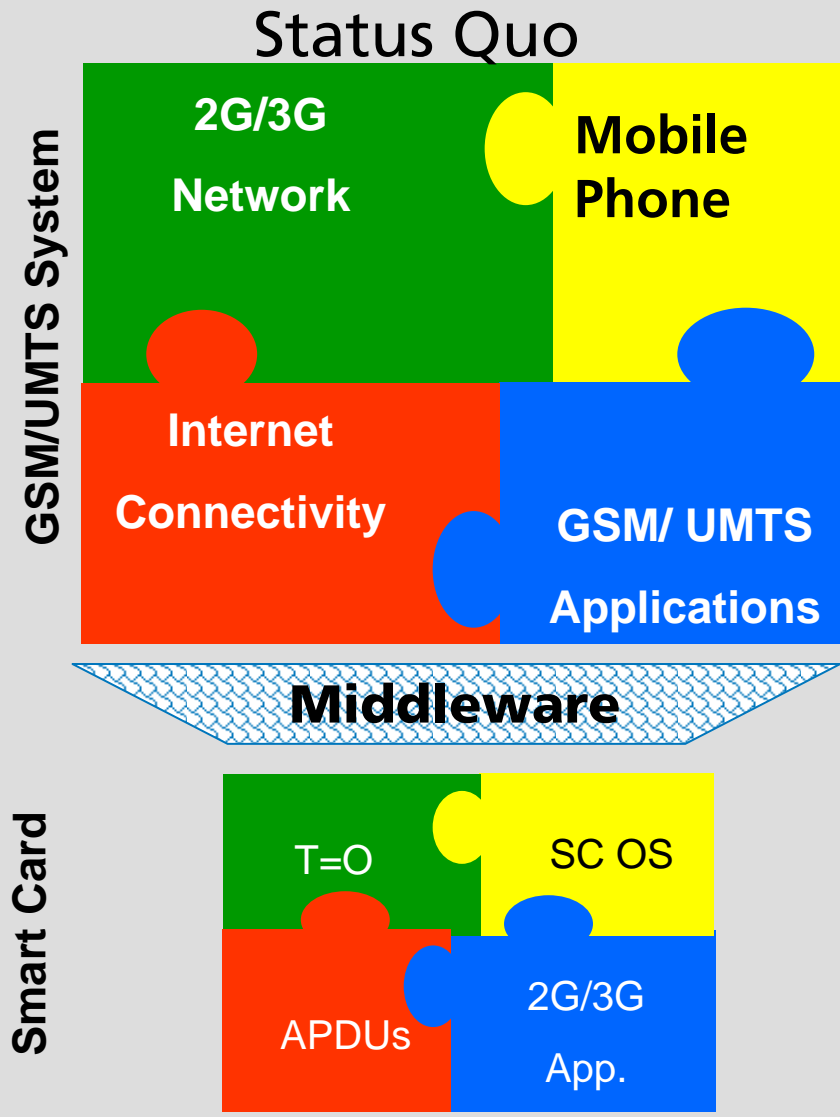
- **The Smart Card becomes fully network enabled**
- **The Smart Card can act independently as network node (no master slave communication as in ISO7816 specified any longer)**
- **The Smart Card offers security/web services based on the IP protocol**
- **The Smart Card becomes more than an authentication token, because it can directly participate in the Internet traffic**
- **Not least, but not least: From the Internet point of view the Smart Card world is "proprietary" (T=0/1, APDUs,...)**



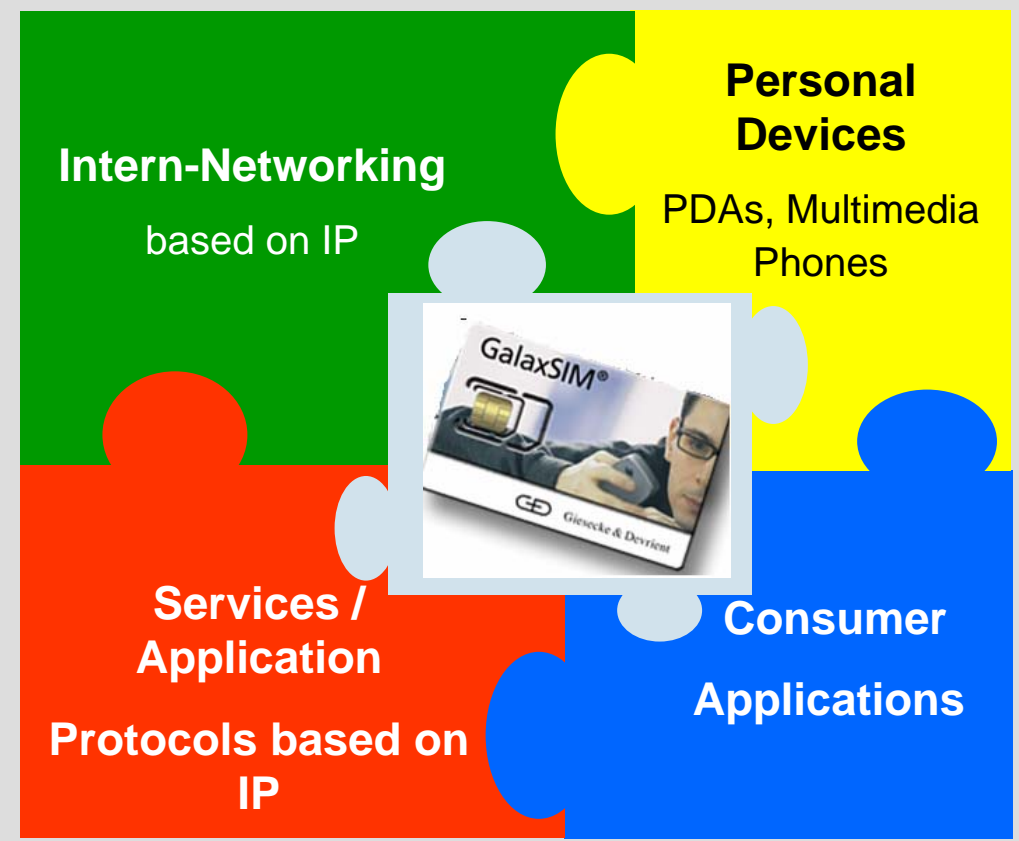
Future Use Cases

- **The Smart Card can directly exchange confidential data with a standard Internet-Server by an end-to-end secured connection (no break of the security chain in the mobile)**
- **The Smart Card triggers actions in the Internet e.g. by a HTTP-Request (no more master-slave communication!)**
- **The Smart Card can communicate with other network components via RPC (Remote Procedure Calls) e.g. Web Services**
- **The Smart Card i.e. the Smart Card Web Server can directly display confidential information in conjunction with mTransaction and mCommerce via an Browser on the mobile**

Interoperability and Connectivity



GalaxSIM (Internet Smart Card Model)



Thank you for your attention!

