gemalto

Gemalto:
a leader in Digital security

L. Manteau, Gemalto Industrial relations

ETSI workshop:
Standards & Interoperability
Sophia-Antipolis, Oct 23-24, 2006

Gemalto's presence worldwide

Gemalto was launched on 2 June 2006 from the merge of equals between Axalto and Gemplus

- €1.7 billion (US$2.2 billion) in combined pro-forma 2005 revenue
- 11,000 employees
- 21 production sites, 9 R&D centers, 120 sales offices
- >1500 R&D engineers

Legend:
- Office
- Personalization site
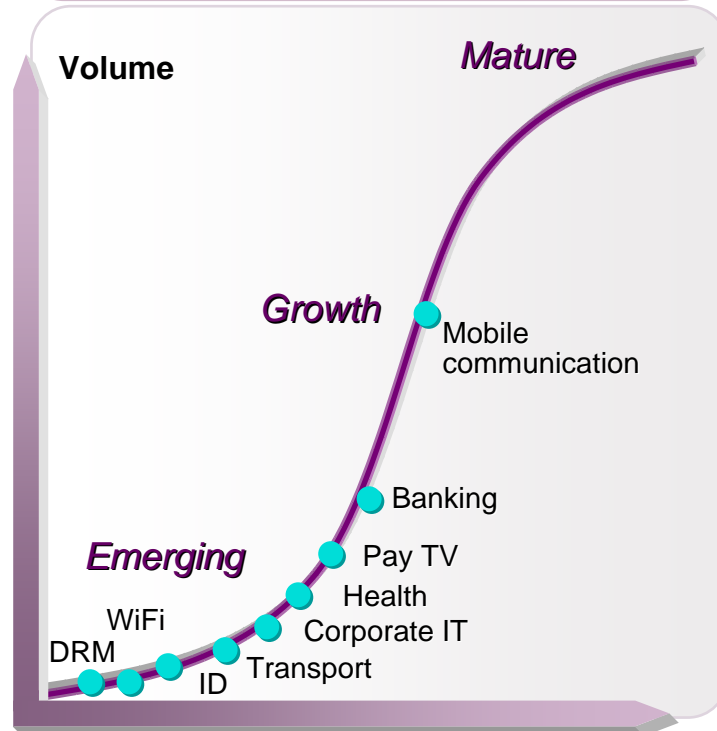- Manufacturing site
- R&D site

Smart card market : global trends

- ✦ The total SIM market is on track to exceed the 1650 Millions units mark for 2006(*)
- ✦ Public Sector cards are on track to become a major contributor to the card industry
- ✦ The Transportation sector has accelerated its endorsement of the value of the smart card
- ✦ Corporate badges with VPN, combined with VoIP and WLAN management have reached a sustainable model to boost deployment
- ✦ Pay TV and DRM expected to represent significant market value in the coming years

Kunits

	2003	2004	2005	2006	2007	2008

■ Memory
■ Micro
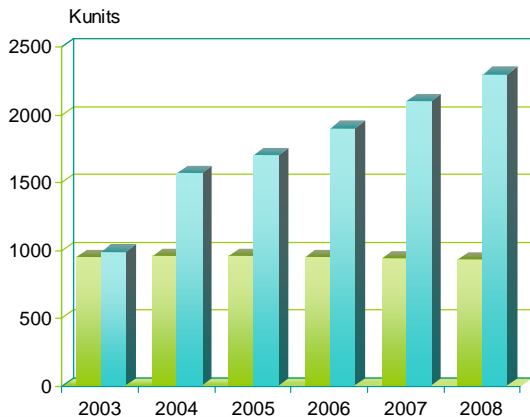
- ✦ A **global market** based on **European technology** and stakeholders

(*) source: Eurosmart (**) source: Gemallto

Volume

Mature

Growth — Mobile communication

Banking

Emerging — Pay TV

Health

WiFi — Corporate IT

DRM — Transport

ID

Market trends in Mobile Telecom : premium service delivery over mobile networks
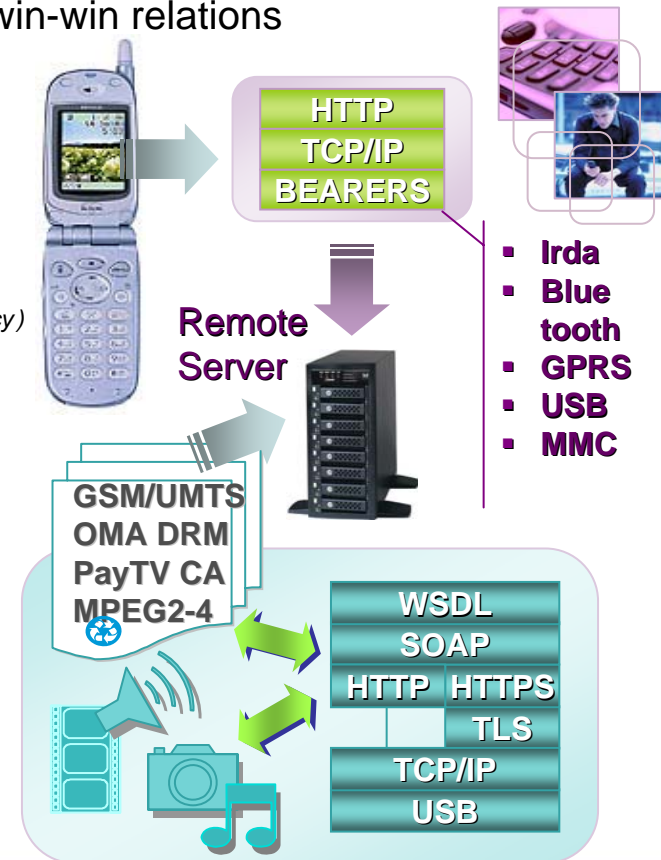
✦ **A highly competitive European smart card industry**

✦ **A complex ecosystem...**
- Multiplicity of actors in the value chain, from content providers to end-users
- Necessity to develop flexible business models enabling win-win relations

✦ **with new technology trends...**
- **High memory capacity to store securely critical objects**
  – 128MB Flash and higher (up to several GB flash) on new 32bits µP
- **High speed protocol between hosting device & card**
  – E.g. BIP, USB IC (12 Mb/s), MMC, NFC
- **Built-in HTTP(s)/IP connectivity**
  – Enabling user browsing of personal & service attributes *(ease of use, privacy)*
  – Secure end to end dialog with remote servers
  – IPV6 underway
- **Web service approach support**
  – Complete Web service stack
  – Federated ID management
- **Possible on-card encryption/decryption**
  – MPEG2 right now at prototype level
  – MPEG4 still challenging

✦ **... requiring win/win partnerships**
- **to reduce investments and R&D costs (critical mass)**
- **to minimize risks on new developments**
- **to prototype innovative solutions**

HTTP
TCP/IP
BEARERS

Remote Server

- **Irda**
- **Blue tooth**
- **GPRS**
- **USB**
- **MMC**

GSM/UMTS
OMA DRM
PayTV CA
MPEG2-4

WSDL
SOAP
HTTP HTTPS
TLS
TCP/IP
USB

Strong Research & Development

✦ Worldwide R&D organization
  ▪ Over 1500 engineers
    and software developers

✦ Specific areas of expertise
  ▪ Security technology
  ▪ Cryptology
  ▪ Advanced operating systems
  ▪ Microelectronics technologies
  ▪ System Architects in mobile com,
    banking, national and corporate ID

✦ High levels of investment
  ▪ USD 130 million (Gemplus and Axalto)
    invested in R&D in 2004

✦ The largest patent portfolio
  in the microprocessor card industry
  ▪ 2,150 patents
  ▪ approx. 50 initial filings every year

International cooperation : R&D partnership strategy

✦ Strong participation in National, Transnational and EU R&D cooperative projects funded by Public Authorities

  ▪ **IST FP6** program : InspireD, eCrypt, Re-Trust, Mosquito projects

  ▪ **Eureka** clusters: **MEDEA+, ITEA, CELTIC, EURIPIDES**

  ▪ French Competitiveness clusters: **System@Tic**, **TES**, **SCS**

  ▪ ANR projects: **RNRT, RNTL, RIAM, Oppidum**

  ▪ **All** framework

✦ Strong complementarity looked at between R&D and business partners

  ▪ Silicon founders, Telcos, Service providers, SW companies

✦ Coherency with internal technology roadmap

✦ Coherency with standardization approach

  ▪ Onom@topic :
    citizen card: ECC reference implementation
    mobile com: SWP demo to support NFC

  ▪ ESPASS-IS : USB full speed on card demonstrator

Mobile telecommunications
A dramatic scope extension

✦ Boosting the performances of smart cards
- high speed communication protocol
- support of mass storage
- support of HSDPA

✦ Opening the cards to the IP world
- Implementation of TCP/IP on board
- Web server in the card
- Improvement of ISIM (equivalent of SIM in IP mobile)

✦ Push further the security offered by card-based solutions
- Secure channel for trusted services between handset and card
- Generic key provisionning

✦ Impose the smart card as a major convergence enabler
- Contactless capability in mobiles
- Authentication on fixed networks
- Reinforce the role of cards in CDMA
- WLAN/WIMAX connectivity

Mobile telecommunications
New application domains

✦ **Device Management**
- Smart Card to provide continuous provisioning of configuration and service parameters
- Look and Feel Customization to update / modify the User Interface

✦ **Digital Rights Management**
- SRM (Secure Removable Media): Secure token, such as SIM to port media rights across handsets

✦ **Mobile TV**
- Content protection for Broadcast media (such as TV) controlled by the card
  - Pay per View with replay counter, Pay per Time, Consumption based subscription
- Provision of Electronic service guide features

✦ **Data Synchronization**
- Solutions for synchronization of data between card(s) and handset(s), e.g.: phonebook.

gemalto^x

Digital ID and transversal standards

✦ **Digital Identity application field**
  ▪ Worldwide standardisation projects
    – electronic Passport (ICAO)
    – driving licence
    – e-Health (+ directives at CEN)
  ▪ European citizen card
    – Protection Profile for e-signature

✦ **Transversal standards**
  ▪ Java Card:
    – switch from APDU/applet model to TCP/IP/servlet model
  ▪ Global Platform:
    – GPD/STIP proposal for trusted environment in mobiles
    – card & system packaging for deployments in ID

How to ensure win-win partnership through standards

✦ develop a medium & long term vision before electing consortia and cooperative programs (exploratory research program, IST, ANR,...)

✦ plug-in a standard vision in the course of a cooperative project

✦ participate to the work done in ETP (in the perspective of the FP7)
  ▪ ENIAC, ARTEMIS, EPOSS,...

✦ follow-up the evolution of JTI (e.g. possible merge with MEDEA+)

✦ nevertheless, Gemalto statements to be shared
  ▪ timing discrepancy between R&D programs, product life cycles and elaboration of standards is a real issue (how to adapt standards approach to real business?)
  ▪ interoperability is a critical issue to be looked at closely either from our own perspective (e.g. 1 To 1 relationship with handset makers) or through PLUGTESTS^{TM}
  ▪ role of ETP to be precised as a catalyst/enabler for EU RTD projects and to be the basis for new standard proposals
  ▪ do we address a global market with individual performance/ROI in mind or EU competitiveness in mind? The answer partly depends on EU and national support to the industry initiatives.

Thank You !