

# Agenda

- ✦ Smart card figures
- ✦ Smart card technology roadmap
- ✦ Future needs
  - New application context
  - Silicon
  - Module
  - Packaging
  - System level environment
- ✦ Recent wins
- ✦ Conclusion

# Smart Card figures

## Telecoms: The first large smart card application

- ✦ About 1.5 billion SIM cards are deployed each year



## Banks: Smart cards secure financial transactions

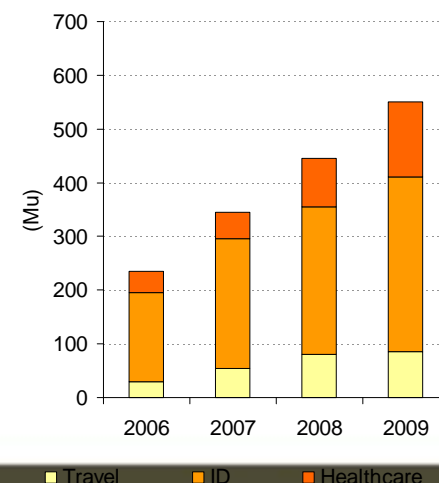
- ✦ EMV migration: 100 countries have already partially or fully migrated
- ✦ Contactless payment is becoming a reality for small transactions, 10 million cards already issued in the USA and Japan



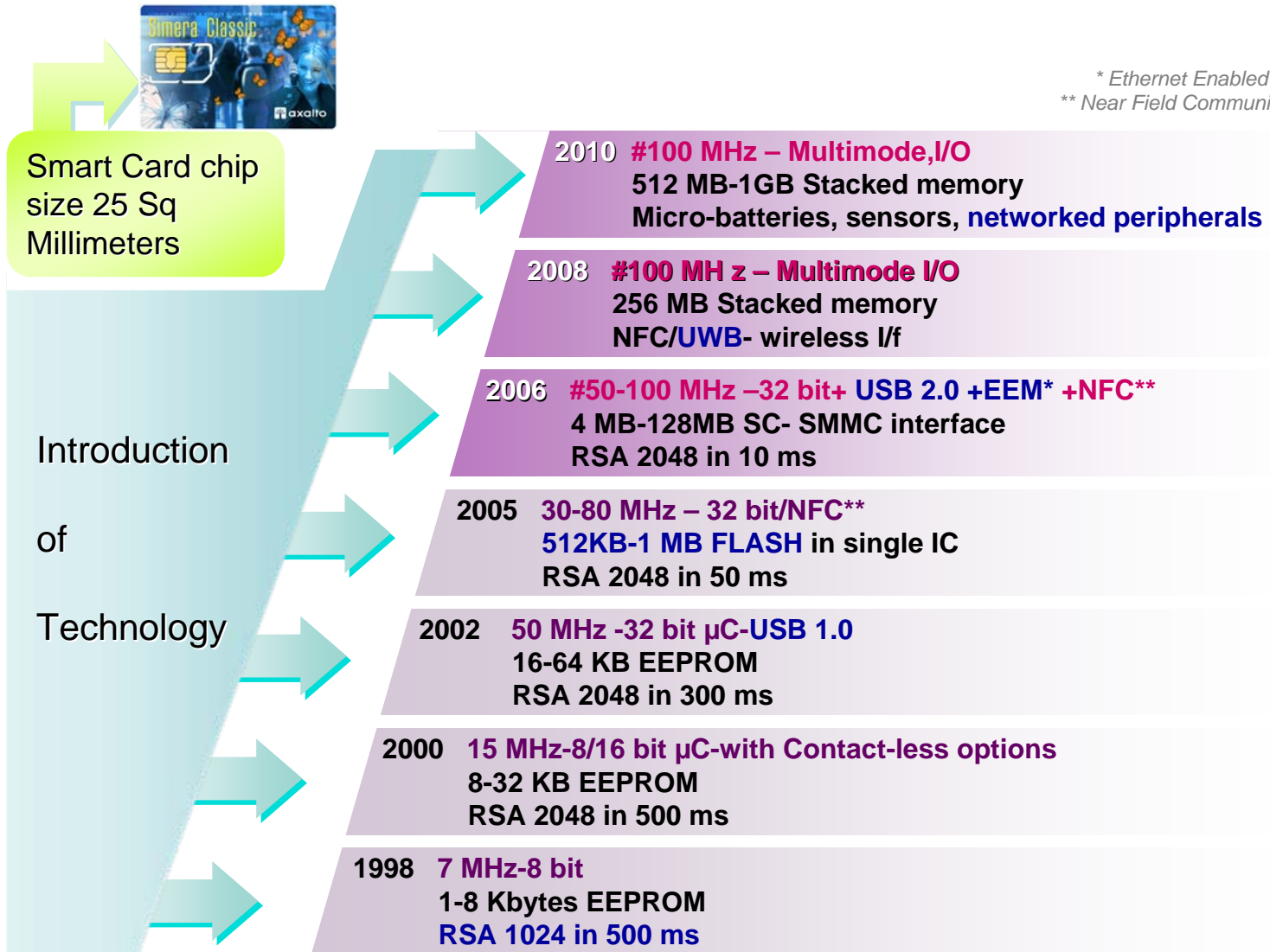
## Identity: Widely-used since 2002

- ✦ ePassport: 2007 - 30 countries already
- ✦ National ID cards, More than 15 countries have adopted an electronic ID card
- ✦ Health care system cards: a proven model, France, Germany, Austria, China, Slovenia etc.

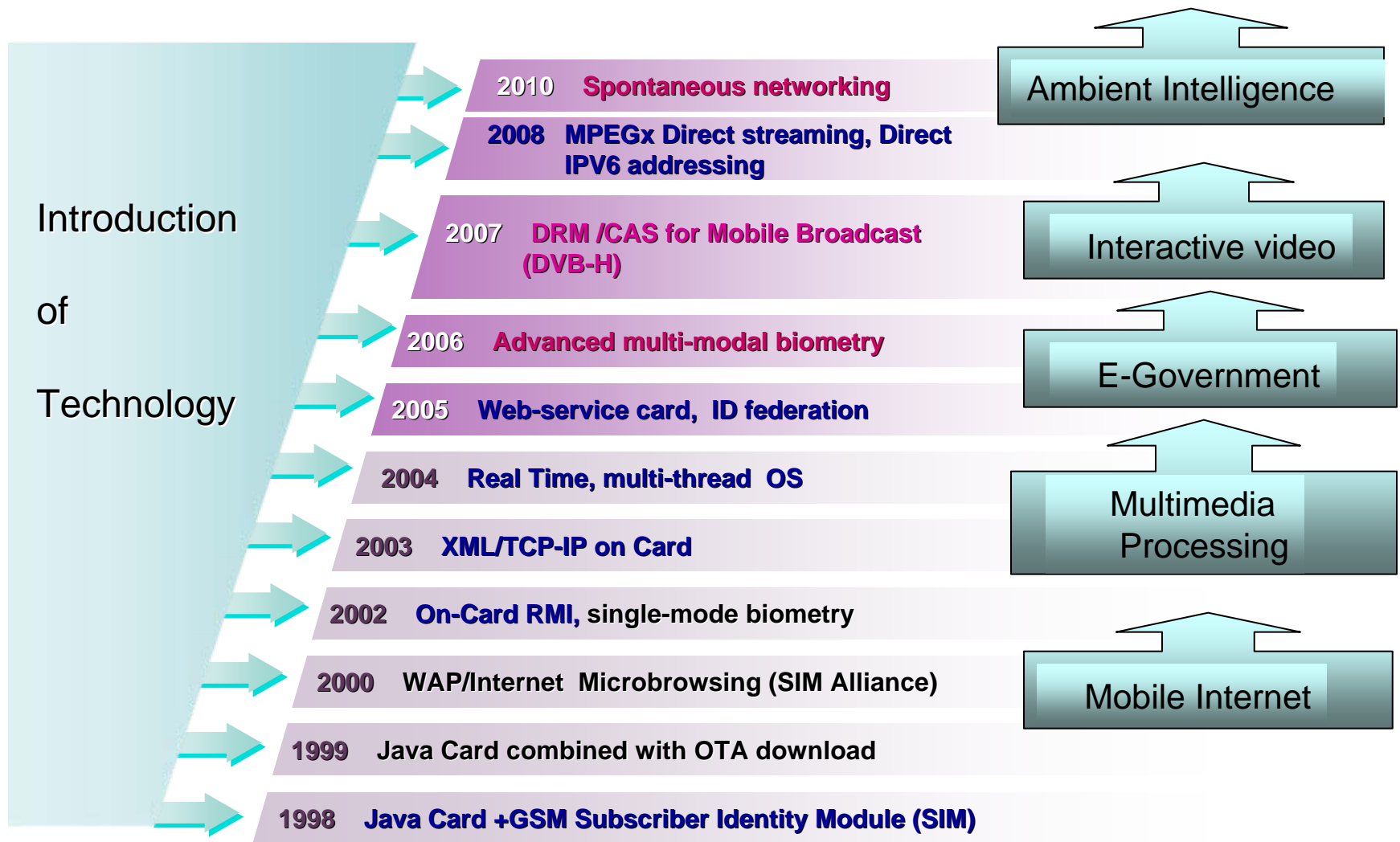
Secure Identity Documents  
Deployment WorldWide (Mu)



# Smart Card Hardware: More Moore and more than Moore

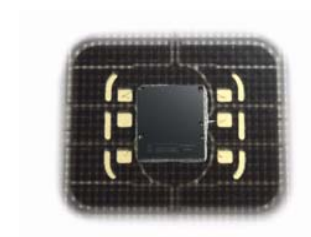
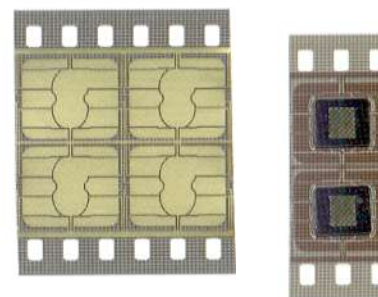
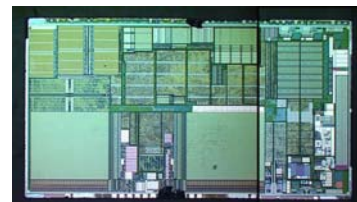


# Smart card: Software innovation, past and future



# Future needs: density - security

- ✦ New application context
  - Enhanced functionality, multi-application
- ✦ Silicon environment
  - New SOC structures
- ✦ SIP Packaging technologies
  - Die to wafer stacking
  - New form factors
  - System level aspects
  - New module and variants
- ✦ Security of the finished good
  - Against destructive and non-destructive attacks



# New application context

- ✦ Enhanced functionality, multi-applications
  - Enable **more functions** in always reducing volumes
  - Increase the **secure storage capacity**
  - Increase **communication speed** between the « card » and remote servers or data-bases
  - Increase the **security of accesses** to servers and processed on-card assets
  - Offer a better **flexibility at communication protocol** levels (ISO, USB, NFC,..)
  - Re-enforce the **physical security, reliability and life-time** of smart-platforms requested by key market applications (Mobile Communications, E-ID programmes, Pay-TV,..)



# Silicon environment

## ✦ Continuous increasing of clock frequencies ( 32 bit CPU)

- Optimal dimensioning of the silicon platform along 4 major axes: CPU, Storage, I/O, Bandwidth
- Power consumption management

## ✦ From large to very large secure data storage

- From several 100 KB to MB/GB
- EEPROM => Flash => PCM and/or MRAM

## ✦ Complex hardwired functions (dedicated coprocessors, state machines, anti-tampering sensors preventing fault insertion)

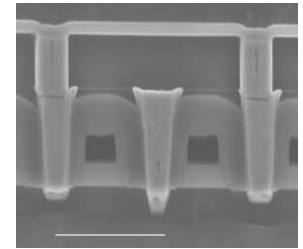
- Up to 50 sensors on most complex processors available today

## ✦ Optimal management of computational power, peak and average power consumption, management of lower noise immunity

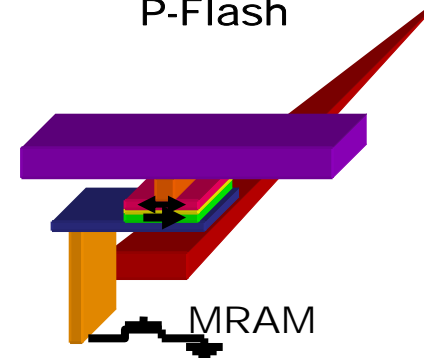
- Not only a functional but also a severe security challenge
- Decoupling and filtering necessary
- Critical for all contact-less applications

## ✦ Heterogeneous integration

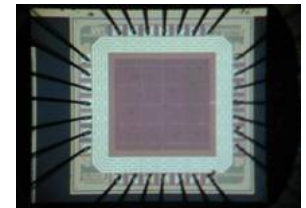
- High-density logic, RF blocks, analog sensors, large embedded SRAM and NVM, asynchronous logic, on-chip remote peripheral controllers,
- Smart cards chips are becoming more and more complex SOC's or SIP's



P-Flash



MRAM

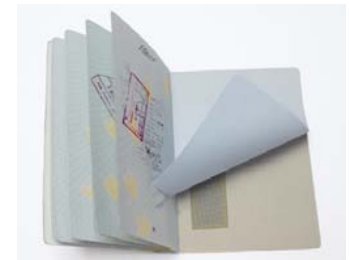


Asynchronous

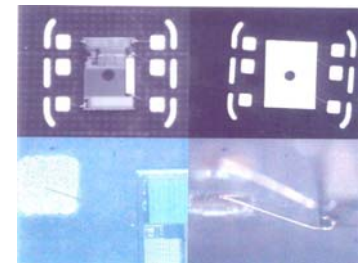
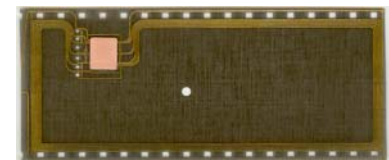
# Packaging issues

## ✦ New form factors and technologies

- **New 3FF** for SIM cards (new standard for Mobile SIM cards)
- **New technologies** for E-Id: (passports, visas)...
- **Die stacking** (CPU et large storage memories: > 1 GB)
- **Passive components** (capacities, SMT, energy sources)
- **Ultra-short embedded die to die interconnect** (with enforced security)
- Monitoring of **embedded power consumption**
- **Low number** of external I/Os (8 contacts ISO)
- **Floppy substrates** (PCBs, RF antenna connection, plastic screens, OLEDs)
- **Very thin** module thicknesses (a few 10 $\mu$  for laminating)



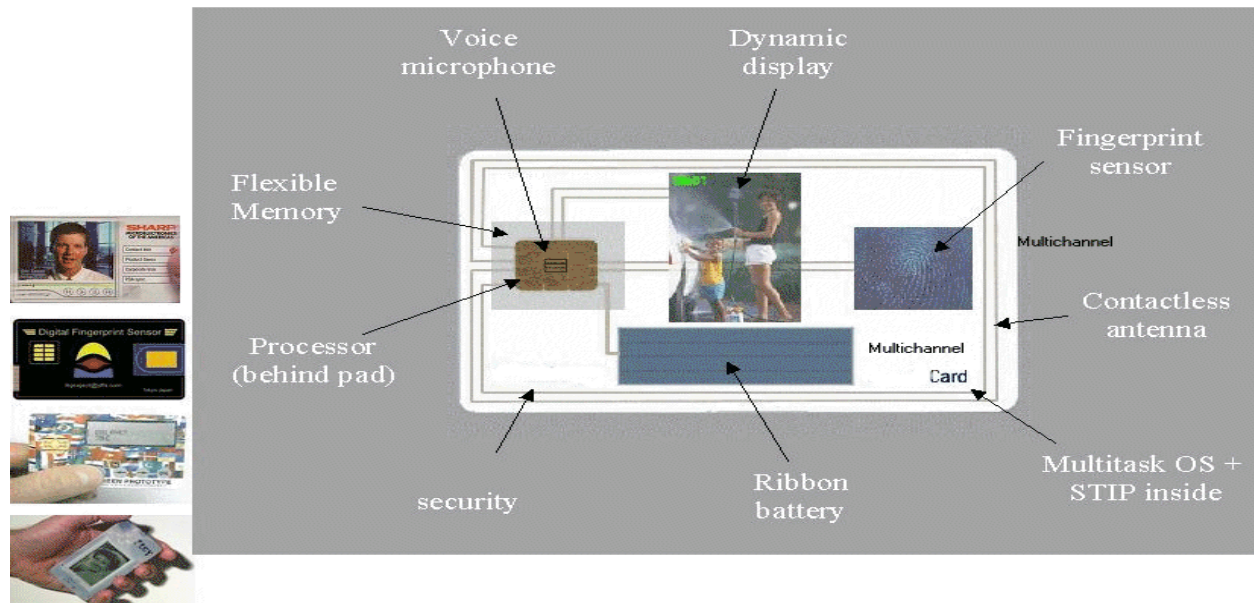
Passport



# New constraints: system level integration

- ✦ Global approach needed
  - at Silicon, at embedded SO,
  - at « packaging » and manufacturing levels

## Smart card becoming a computer ?

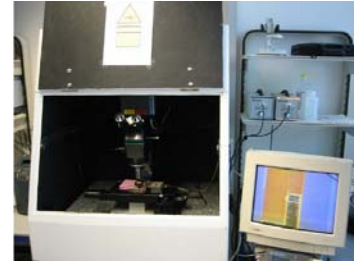


- ✦ .....with new management approach for the associated security risks
  - Design methodology
  - New security challenges

# New security challenges on smart cards

## ✦ Prevention against invasive attacks

- Active layer protection by robust die sealing and attachment
- Inter-die link protection for multi-die structures (through suitable place and route)
- Embedding of energy micro-sources (micro-batteries ) enabling a non-destructive control of module and event dating



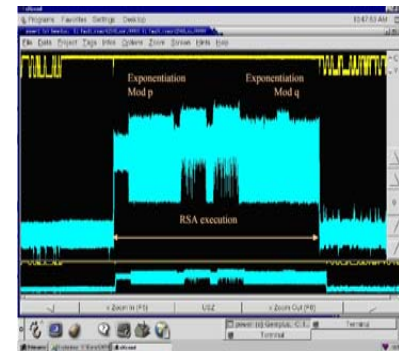
## ✦ Prevention against non-invasive attacks

- Perturbation of consumption current analysis (SPA, DPA) through the simultaneous operations of the stacked dies
- Electromagnetic emission control
- Counter-measures against fault-injection attacks (3D active topologies, ad-hoc surface processing.... )



## ✦ Prevention against combined attacks

- Simultaneous perturbations of both IC and modules



# Gemalto's strategy in action: recent wins

## ✦ Mobile TV:

- MTN in **South Africa**; T-Mobile in **Czech Republic**

## ✦ Contactless mobile/transport

- **French** mobile communication operators and RATP

## ✦ Secure on-line transactions

- **UK:** Devices and services to Barclays Bank

## ✦ Contactless payment

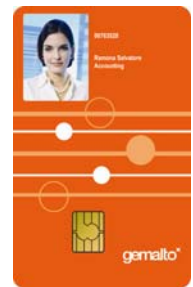
- **Taiwan:** China Trust Commercial Bank combi card launches

## ✦ Enterprise strong ID authentication

- Microsoft Vista adopts and supports our .NET devices

## ✦ Government ID

- **Estonia:** entire e-passport value chain
- **Oman:** complete turnkey solution for national ID
- **US:** supply of e-passports to GPO



# Conclusions

- ✦ Market dynamics for smart card systems requires a permanent revisiting of functionality and security
- ✦ Changes required concern not only the classical silicon environment but also the complete packaging and system integration chains
- ✦ Mobile Multimedia is a very strong driver for multi-chip integration
- ✦ New E-ID products are pushing for new system level packaging options with very strong integration between microelectronics and complete physical security
- ✦ There will be many challenges behind us!

Thank you!

Michel THOMAS  
Industrial Relations  
+33 6 86 48 92 08  
[michel.thomas@gemalto.com](mailto:michel.thomas@gemalto.com)





## ARCSIS MICROPACKAGING DAYS 2007

Provence Microelectronics Centre, Georges Charpak Site, Gardanne,  
France

29 & 30 November 2007

Provence Microelectronics Centre – Micro-PackS R&D platform  
Georges Charpak Site – Gardanne - France



ARCSIS MICROPACKAGING DAYS 2007

[WWW.ARCSIS.ORG](http://WWW.ARCSIS.ORG)

This event will take place on **November 29 & 30, 2007** and is open to national and international microelectronics key actors working in this field. This event will be as well the occasion to visit the new R&D platform "ARCSIS-MicroPackS" dedicated to advanced micropackaging solutions.