

Next Generation Smart card: new features, new architecture and system integration.

Results from Inspired WP1.3

Denis PRACA – Research scientist

GEMPLUS System Research Lab



Today we will speak of...

- New smart card uses cases
 - Moving toward Trusted Platform Device
- Introduction of new features
- Implication on SC operating system
- System integration
- Exciting and bright future... not so far !

INSPIRED work methodology: Use cases and profiles

Application areas for TPD

- Work methodology based on market segment and form factors (profiles) cross analysis
- User panel feedbacks used to improve definitions and requirements

	S3	S4	M3/M4	M8
Application Area's of TPD's	SIM	MSC	Token	Smart Card
Mobile Telecommunications	X	X		
DRM (Pay TV,)	X	X	X	X
Enterprise Security (PKI)	X		X	X
e-Government (electronic ID)				X
Ehealth		X	X	X
Banking / Payment	X		?	X
Retail / Loyalty	?		X	X
Mass Transit (Ticketing)	X		?	X
Access Control	?		X	X
others ?	?	?	?	?



SIM Profile

- New services targeted:
 - Secure and trusted network operation including traffic encryption and web services delivery
 - Easy to use value added services
 - Custom and private user data management

- New technical features needed:
 - Increased storage capacity
 - Improved input/output regarding to the network bandwidth and protocols and to the local processing capabilities
 - Bandwidth must also be adjusted according to user experience (Ex: Access time to card data storage)
 - Higher processing power to enable larger and easy to develop applications
 - Support of contactless communication



Mass Storage profile

- Mass storage cards are expanding their capabilities by adding smart card functionalities:
 - SD card promotes smart SD for mobile commerce
 - Secure MMC 2.0 specifies OMA DRM application and Javacard/GP functionalities
- Strong slot presence in PDA, mobile phones, cameras (Wifi connected!)... open new opportunities and new applications (DRM, secure personal storage,...)
- Mass storage technologies may also become of strong interest in traditional smart card markets like mobile phone:
 - Re use of widely deployed interface
 - NAND flash assembly and management (Flash Translation Layer)
- Need external memory interface like I²C, SPI, NAND Flash interface with throughput ranging from 3Mb/s up to 300Mb/s

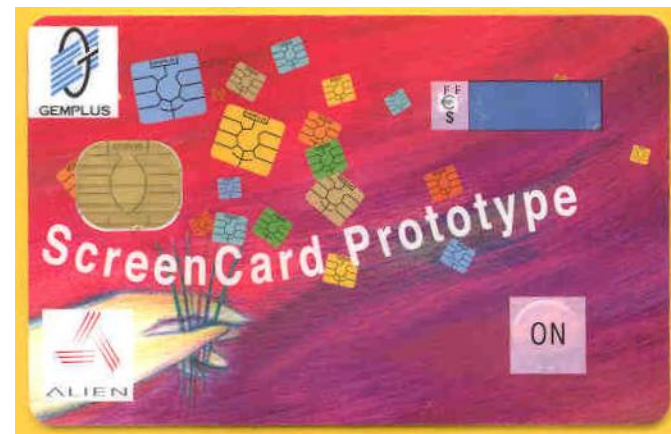


Token profile

- USB token is one of the most successful product for IT users
 - Mainly used as a removable storage
- Growing market for corporate security (VPN access)
- As for mass storage card, new comers may introduce advanced security features like in U3 consortium: turning a USB flash drive into a USB smart drive

Smart card profile

- Continuous improvement of smart card technologies by increased processing power, memory and new external interfaces
- Addition of display, buttons, battery, oscillator, biometric sensor, microphone, speaker, camera... on a smart card
 - Need new features like power management, power source switching
- We are moving toward real terminals



What are the technologies needed for each profile ?



Sub-class		relevant TPD profile	Multi Components					Host interface				UI	Power			
Characteristics (X) & Options (O) of relevant TPD profile			High density memory	Co-processor	Biometric sensor	Display	Knobs	Use of ext. antenna	ISO 7816	USB	MMC	ISO 14443 or NFC	Autonomous	Host-based	Onboard	Offboard
SIM	S3	System on SIM	X	O					X	O	O	O		X		X
MSC	S4	Contact MSC	X	O	O					O	X	O		X		X
Token	M3	System on Token	X	O	O	O	O			X				X		X
Token	M4	Combi SoT	X	O	O	O	O			X		X	O	X	O	X
SmartCard	M8	System on Card	X	O		O	O		X	O		O	O	X	O	X

New external interfaces technologies



USB interface

- Widely deployed in the PC world
- Only full speed (12Mb/s) and high speed (480Mb/s) are considered
- Clock recovery (48 MHz or 1,92 GHz) needed to support USB frame transfer
- High speed is mandatory for mass storage applications
- Token is the first target but InterChip specification is also considered for UICC high speed interface
 - USB power consumption is a big issue in a mobile phone
 - Wide deployment in IT world may reduce the learning curve of the technology



MMC interface

- Widely deployed in PDA and mobile phone together with SD cousin's
- Speed fully scalable from 0 to 416Mb/s depending on clock frequency and bus width (1,4 or 8 bits)
- Mass storage card natural choice and also considered for UICC high speed interface
 - Wide deployment and easy integration will help time to market
 - Scalability will help device manufacturers to target different markets with the same technology



Very large memory

- On chip memory will range from Mega bytes to few tenth of Mega bytes
 - Execute in place possible for some configuration
- From 64Mbytes, external memory configuration using NAND flash seems mandatory
 - No execute in place possible and FTL is needed
 - Up to 60 Mbit/s write speed currently available today



Contactless interface

- Consensus is reach on the need of an external contactless RF front end (CLF) for static cards plugged in a mobile appliance
- Interface between CLF and TPD may use various signaling:
 - A 2 wires dedicated interface
 - A 1 wire dedicated interface
 - Compatible with USB on 8 pins ISO7816-2 module
 - Share TPD VCC signal: the CLF will be in charge of TPD power management for battery powered / emergency mode / battery broken mode.
 - Compatible with MMC interface on 8 pins ISO7816-2 module

New Operating system drives new architecture



Increased memory size

- New operating systems dealing with TCP/IP and multithreading are much more complex than Javacard 2.X
 - Core OS size and RAM needs are increased of about 50%
- More complex applications are permitted by these new OS and may now fully run in parallel
- Increased external communication speed means larger memory buffers



Multi-threading

- Multi-threading is needed by applications developers in order to guaranteed application independence and better performances

- Advanced OS development will be greatly simplified by hardware features like MMU and MCU, fast context switching



Execution of code in RAM

- Just In time Translation: Byte codes are translated “on the fly” by the OS into native machine instructions:
 - Well known technology to combine byte code language flexibility and execution speed of native code
 - Require different security policy
- New memory model based on large mass storage memory
 - Execution in place no more possible
 - Need more RAM and MMU



Memory management

- MMU:
 - Needed to allow execution of large applications stored in mass storage memory
 - Is required to allow transparent management of non volatile memory

- MPU:
 - Increase security of more and more complex OS
 - Needed to protect native application code execution

- DMA:
 - Required for fast transfer between interfaces, crypto engines,...
 - May be replaced by shared memory (Multiple port RAM)

New applications drives new
performances



On the fly cryptography

- Improved interface speed allows our dear marketing guys to think about new applications:
 - Fast encryption, decryption and signatures of documents, emails,...
 - Real time encryption or decryption of streamed data
 - Mobile TV
 - Voice

- Fast symmetric crypto engines will need to be able to process about few megabytes/s



Full Java support

- Business requirements
 - Should enable new (means additional) markets for Java Card
 - Target **32-bit microcontroller architecture with large memories**
 - Closer to mainstream Java
 - **Communication limitations** should be removed
 - Support different kinds of applications

- Technological translation
 - **Multithreaded execution engine**
 - **Objects in RAM**
 - Automatic garbage collector
 - On-card linking
 - CLDC-like core APIs
 - Flexible framework, supporting multiple application models
 - New communication stack using Internet Protocols



Better integration in the infrastructures

- Thanks to full TCP/IP connectivity up to the card, we are able to take part of internet world
- User interaction with the card using standard WEB applications like HTTP browser
- OTA management greatly simplified by standard SyncML, FTP transfer for large files...
 - Throughput greatly improved compared to SMS
- New applications like identity management
 - UICC act as an identity server for all your WEB applications
 - Required to be reachable from everywhere!

Conclusions



Smart card is entering a new ERA

- Technological revolution
 - New interface speed
 - Very large memory
 - Open and powerful operating system
 - Standard connection to the internet world and application class
- INSPIRED is the common view of the whole industry
 - We are working together to impose new standards

Thank you

Q & A session