

Mobile security becomes reality

The Mobile Security Card

Michael Poitner
CTST 2008, Orlando/FL



Giesecke & Devrient

A new 'smart card' form factor

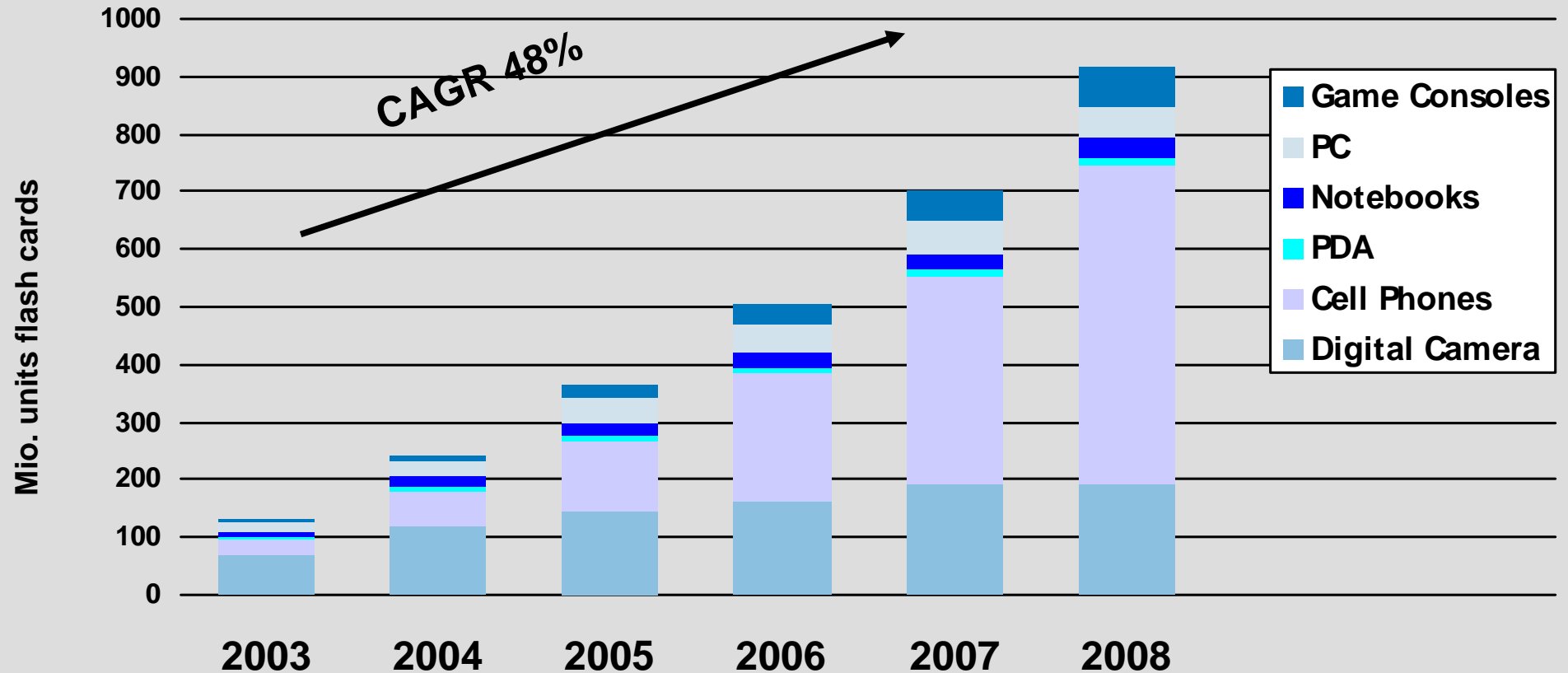


Smart Cards

Secure USB-Token

Secure microSD

Memory card adoption in mobile devices on the rise



Source: Web-Feet
Research

Secure microSD card

Secure microSD card CTST 2008.ppt



Giesecke & Devrient

Mobile Devices today: Connected and „unconnected“ devices



More than 800 models are available on the market in 2007 with slots for removable SD-memory cards.

Mobile Security Card: Architecture Overview

Two-controller architecture

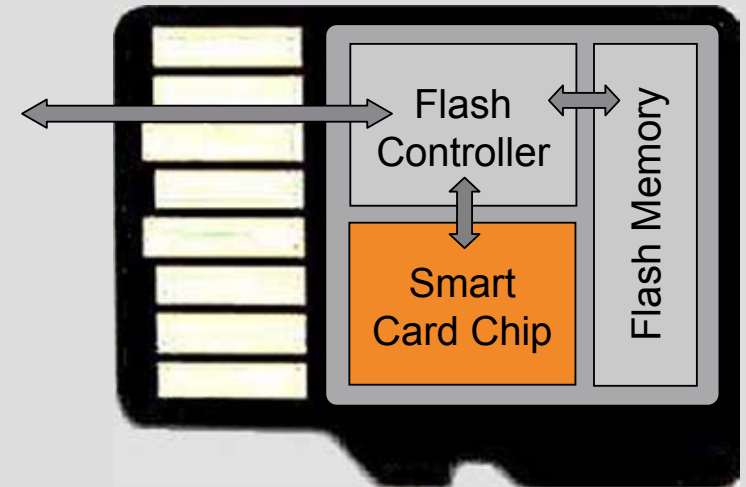
- Flash controller
- Security controller
- Internal I/F: ISO 7816

Access to flash memory

- Using standard SD read/write commands

Access to security controller

- Flash controller acts as proxy (like a smart card reader)
- Smart card APDUs tunneled via specific SD read/write commands
- Two interfaces provided: Mc-EX and Generic Security Interface



Mobile Security Card (MSC) – Key Features

- Java Card 2.2, Global Platform 2.1.1
- EEPROM: 72kByte, Flash Memory: 2GByte
- RSA up to 2048 bits (RSA and RSA CRT)
- AES up to 256 bits
- Hash algorithms (SHA1, SHA256, MD5 and RIPE MD-160)
- Hardware: Common Criteria 5+
- Software: Sm@rtcafe[®] Expert 3.2 (FIPS 140-2 level 3 under evaluation)
- Tools support
 - Application development
 - Lifecycle management



Areas of Application

- User authentication and network access
 - Secure log-on
 - Secure VPN access
 - Email signing/encryption
 - Memory encryption
 - Single sign-on
- One time password storage
- Mobile banking and secure payment
- Contents & rights management



Mobile Security Card provides real smart card security

- Contents of smart card IC cannot be cloned
- Credentials never leave the card as plain text
- Two-factor authentication possible (card+PIN)
 - Strong user authentication and access control
 - No risk of abuse in case of loss
- Enables prevention of frauds, e.g. allows
 - Protection of pay-per-use services
 - Protection of preloaded SW and contents
- High portability of credentials as well as secured data



Mobile Security Card integrates easily into mobile devices

Easy driver integration due to generic interfaces

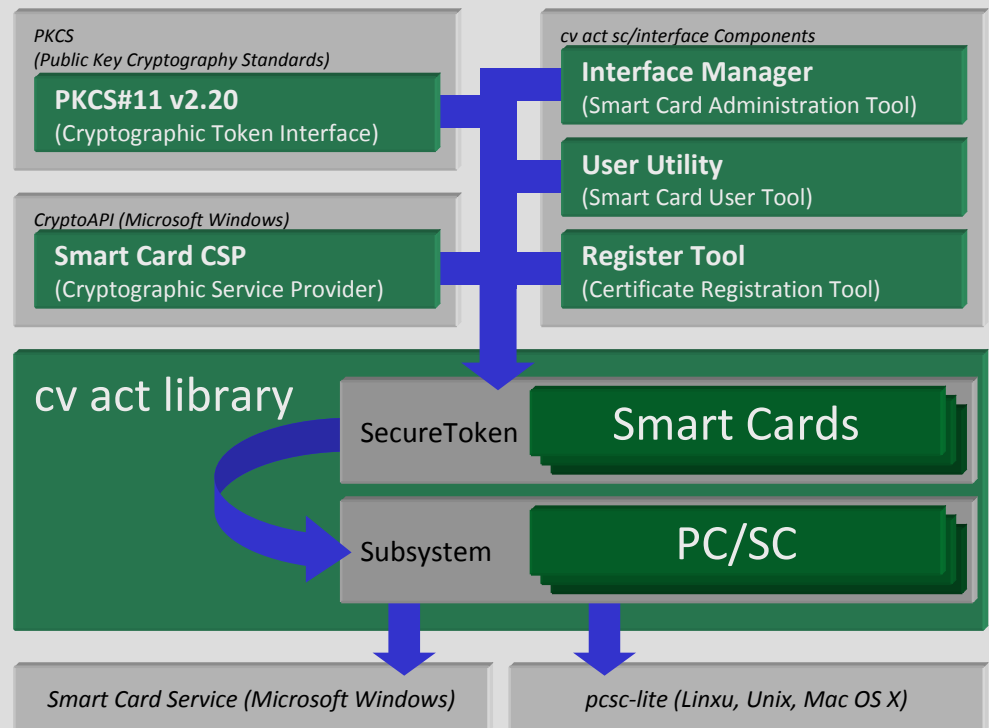
- Drivers available for Windows, WinMobile, Linux, Symbian.
- Consumer installable on Windows, WinMobile, and Nokia Series 60
- Easy integration by OEM on other platforms, supported by G&D.

Smart card middleware

- CSP
- PKCS#11

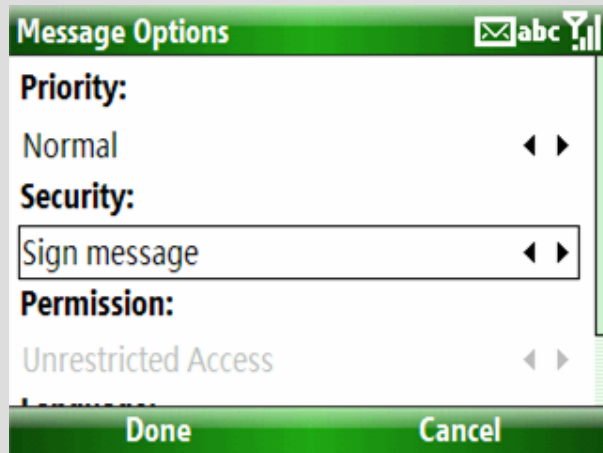
Security software

- Memory encryption
- Email encryption plug-ins
- VPN clients
- OTP clients

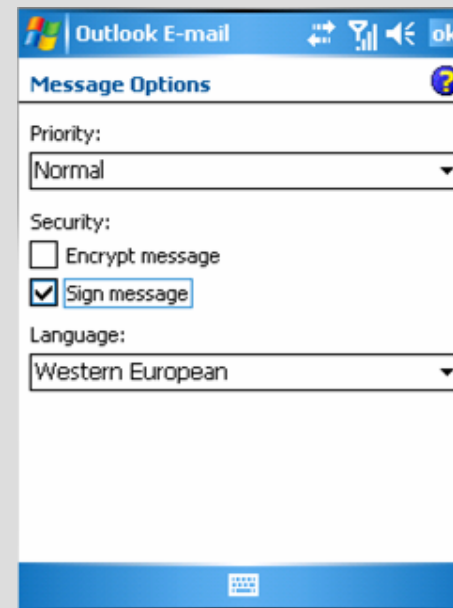


S/MIME support under Windows Mobile

Windows Mobile 6 and 5 (with Messaging and Security Feature Pack – MSFP, AKU2) offer native support for S/MIME



Windows Mobile 6



Windows Mobile 5.0 with
AKU2

Supported Phones (Windows Mobile)

Windows Mobile		
HTC P3600		Windows Mobile 5
HTC S620		Windows Mobile 5
HTC Breeze 160		Windows Mobile 5
HTC Prophet		Windows Mobile 5
HTC Touch		Windows Mobile 6
HTC S 710		Windows Mobile 6
Samsung I600		Windows Mobile 5
Fujitsu-Siemens Pocket Loox T830		Windows Mobile 5
Eten M600		Windows Mobile 5
I-Mate JAMin		Windows Mobile 5
XDA Exec		Windows Mobile 5
Gigabyte G-Smart t600		Windows Mobile 6







Secure microSD card

Secure microSD card CTST 2008.ppt



Giesecke & Devrient

Supported Phones (Symbian)

Symbian	
Mobile device	Operating System
Nokia E65 	Symbian OS 9.2
Nokia E50 	Symbian OS 9.1
Nokia E61 	Symbian OS 9.1
Mobile device	Operating System
Nokia E61i 	Symbian OS 9.1
Nokia E90 Communicator 	Symbian OS 9.2
Nokia E70 	Symbian OS 9.1

Supported Phones (Linux)

Linux

Mobile device Operating System

Quantum OTM 1000 DVB-H Pocket-TV		Linux
--	---	-------

ZTE-G R970		Linux
------------	---	-------

Mobile device Operating System

Aigo DT5200		Linux
----------------	---	-------

Asus EEE-PC		Linux
-------------	---	-------

Thank you for your attention – Questions?



Giesecke & Devrient America, Inc.
New Business
Michael Poitner

Michael.poitner@gi-de.com

Office: +1-650-312-1241

Mobile: +1-571-236-6942