Understanding modern security controllers

- which chip do you need for your identity document?

Ingo Liersch
Infineon Technologies AG
Director Product Marketing
Infineon Technologies at a Glance

The Company

› Infineon provides semiconductor and system solutions, focusing on three central needs of our modern society: Energy Efficiency, Mobility and Security
› Since 1999, Headquarters in Neubiberg (near Munich), Germany
› More than 36,000 employees worldwide (as of Sep. 2016)
› Combined pro-forma revenue of ~6,473 bn €* in Infineon 2016 fiscal year
› 33 R&D locations; 20 manufacturing locations and worldwide sales & support network

Smart Cards

Embedded Security

*non-audited figures
The timelines for the worldwide rollout of passports and eIDs

- Since 1999 first proprietary eID solutions (e.g. Finland eID)
- Triggered by 9/11 in 2001 Visa Waiver countries introduced ePassports
- With introduction of ePassports upcoming trend to use eMRTD applet in eID

The main reason for chips has not changed the last 18 years ago – to secure your credentials. But this many years of development and the ongoing fight against attackers has dramatically changed and improved security controllers.
Chips in Passports and ID cards enable automated gates, increase security and tie the document holder and the document together (biometrics)

Why chip? There are reasons for it!!
The triangle of requirements for security controller 10 years ago for eID / ePassport

**Security**
- Sensor based security
- Strong dependence of HW – SW interaction

**Memory**
- Chips based on EEPROM and ROM
- Memory size of 32 – Kbyte enough

**Performance**
- 8bit architecture enough
- Asymmetric CoProcessor needed (RSA up to 1024 bit)
- Contactless Speed @ 106 – 424 kBit/s required
The triangle of requirements for a modern security controller for eID / ePassport

**Digital Security**
- Comprehensive error detection
- Self-checking dual CPU

**Flash Memory**
- Flexibility & short time to market
- Memory size of up to 1MB

**Performance**
- 16 or 32bit architecture
- RSA key length >= 2048bit
- Very High Bit Rate Contactless Speed @ 6.8MBit/s required

Requirements are met by SLE78/SLC 52 security controllers

* registered Trademarks of Infineon Technologies
**Application specific requirements - Recommendations**

**ePassport Chip**

**ePassport chip:**
- Contactless performance: Minimum 848KBit/s; for use cases with higher amounts of data (future ePass with eVisa, eStamp) VHBR with 6,8MBit/s is recommended
- Minimum memory 80KBytes: gives flexibility for SAC or EAC implementations
- Security controller itself should Common Criteria EAL6+ certified
- Compound certification of HW / SW / ePass application EAL 5+ or EAL4+
- Robustness for 10 years
- Use chips from the well-known chips suppliers for ePassports

**eID chips**

- Use your ePass chip! – with increased memory for multi – applications – make sure that such a family concept is available

Source: Infineon
<table>
<thead>
<tr>
<th><strong>Wrap-up</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chip in eDocuments are one of the most important security features</strong></td>
</tr>
<tr>
<td><strong>Chips tie the document holder and the document together by biometrics</strong></td>
</tr>
<tr>
<td><strong>ePassports enable Automated Border Control Gates</strong></td>
</tr>
<tr>
<td><strong>Contactless performance of ePassports is important and will become essential in future (VHBR)</strong></td>
</tr>
<tr>
<td><strong>Digital security (dual CPU security concept helps against increasing security attacks</strong></td>
</tr>
<tr>
<td><strong>Only use Common Criteria certified chips (EAL6+ recommended)</strong></td>
</tr>
<tr>
<td><strong>Use your ePassport chip also for your ID – maybe with more applications</strong></td>
</tr>
</tbody>
</table>
Part of your life. Part of tomorrow.