

OCOVA 2006

Forum Vie Quotidienne

« Secure Your Embedded Devices »

Michel Bartosik

EMEA Business Development Manager

ATMEL Rousset





The Electronics Industry Faces Major Concerns Today

■ HIGH-TECH GOODS COUNTERFEITING

- Cell phones, computers, printer cartridges, ...
- \$100 B lost each year



■ MULTIMEDIA CONTENT COPYING

- Music, movies, software, ...
- Hackers regularly crack Digital Rights Management (DRM) systems, see the famous CSS (Content Scrambling System) algorithm used for DVD copy protection



■ IDENTITY THEFT OF WEB APPLICATIONS

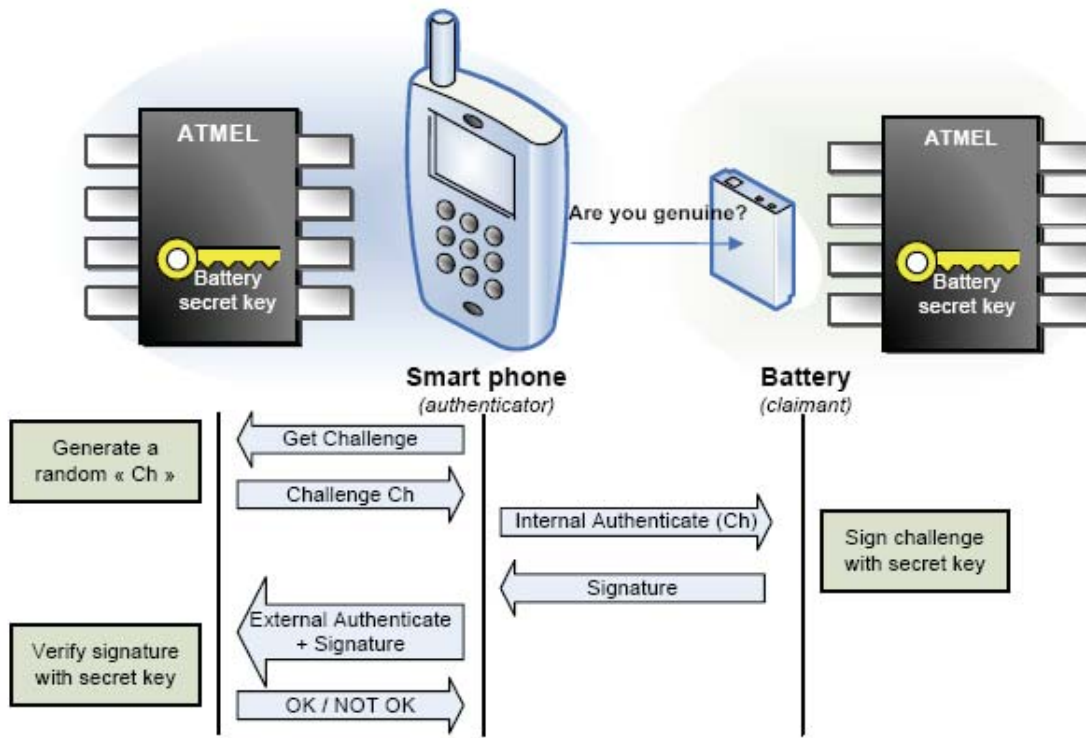
- Banking, shopping, ...
- \$55 B lost in 2005 on the US alone
- Online attacks rare, phishing exponentially growing



Secure Solutions (1/3)

■ SECURE YOUR HARDWARE – ANTI-CLONING SOLUTIONS

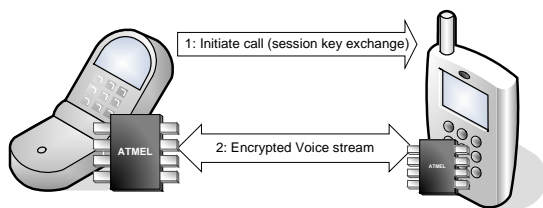
For instance, cell-phone battery anti-cloning system



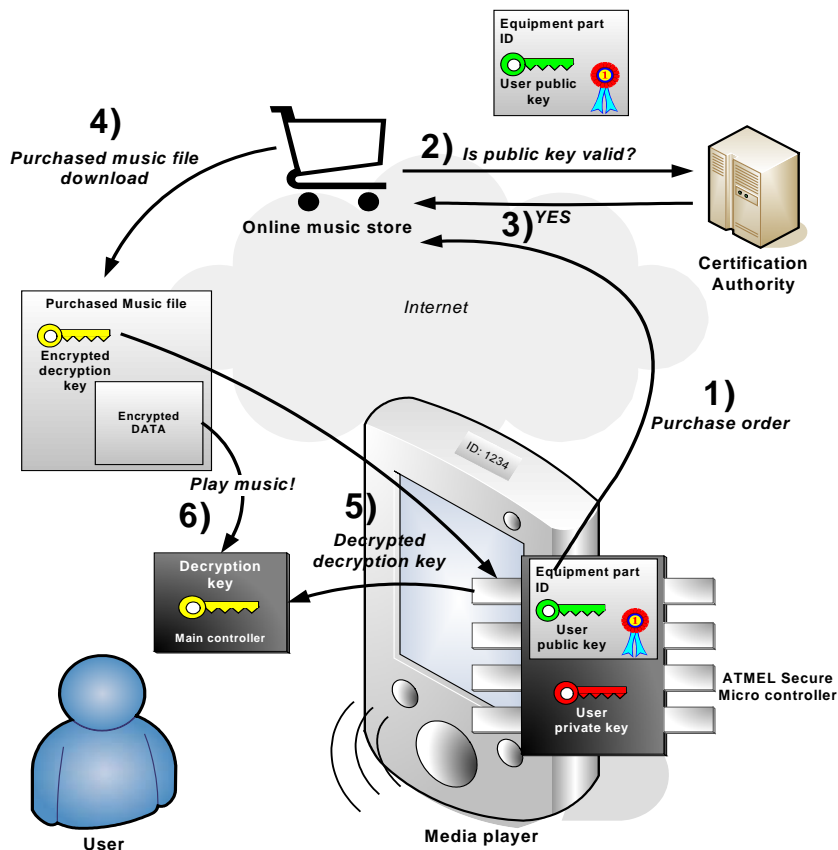
Secure Solutions (2/3)

■ SECURE YOUR DIGITAL CONTENTS – DRM AND SOFTWARE COPY PROTECTION

- DRM for instance, media player
- On-the-fly encryption



- Software protection





Secure Solutions (3/3)

■ SECURE YOUR PRIVACY – MULTI-FACTOR USER AUTHENTICATION SOLUTIONS

■ USB tokens common features

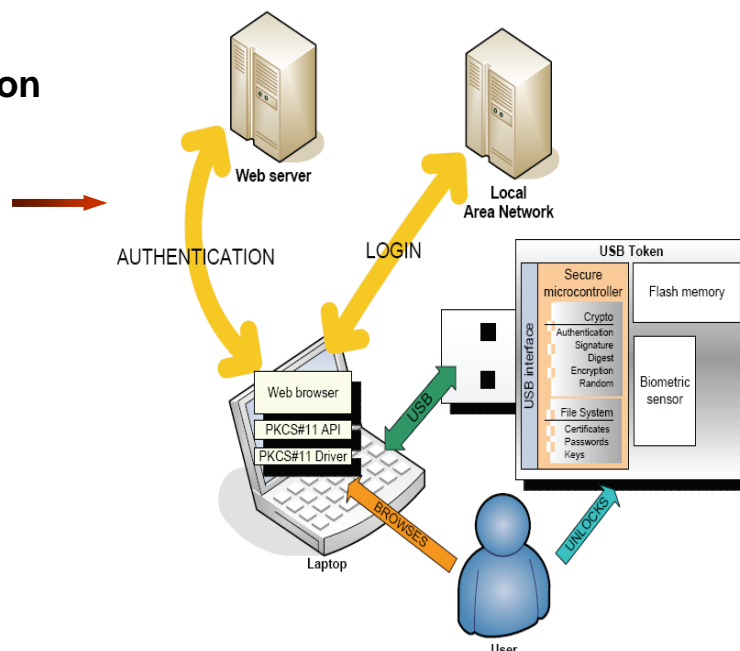
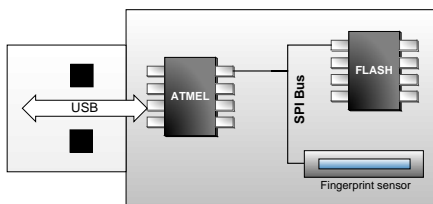
To perform

- challenge response authentication
- One-time password generation
- Token holder authentication

Hardware token common features

- Single sign-on
- Certificate storage
- Token sharing
- PKCS #11 API (RSA™) or MS-CAPI (Microsoft®)

■ Implement a high-end USB token





Chip Solutions Brought by Atmel

In addition to chip families used for smart cards, electronic passports, Pay-TV terminals or trusted electronic transaction terminals (POS, PINPads and Health Card Readers) :

- **Turnkey solutions for the solutions explained herebefore**
 - **More-flexible interfaces than TPMs with a lower PIN count**
 - **Various communication interfaces including SPI and USB**
 - **Low power consumption**
 - **Embedded firmware (crypto. algo., crypto. protocols, communication security, administration modes, ...)**

