Smart Cards

Towards a modern run-time platform

Thorsten Kramp & Michael Kuyper
IBM Zurich Research Laboratory

Who, Where, and When

•	Lecture:	Thorsten Kramp	`thk@zurich.ibm.com`
		Where?	ETZ E9
		When?	Mo, 8-10am
•	Exercises:	Michael Kuyper	`mku@zurich.ibm.com`
		Where?	ETZ E7
		When?	Th, 4-5pm

Exercises

- Hands-on programming exercises
  - *voluntarily, submissions will be corrected*
  - *"official" solutions will be made available online one week later*
- Eclipse IDE
  - *version 3 for either Windows, Linux, or MacOS X*
  - *free download from* `www.eclipse.org`
- JCOP Tools Eclipse Plug-In
  - *includes simulation environment*
  - *free download from* `www.zurich.ibm.com/jcop`
- Smart Cards and Readers
  - *sample smart cards will be provided by IBM*
  - *smart-card readers will be provided by the ETH*

TOC

1. Introduction

   hardware overview, communication modes and protocols,
   classification of smart-card operating systems

2. Software and It's Interplay

   basic machinery, memory management, atomicity and transactions,
   object-oriented programming w/ resource constraints

3. Security and Cryptography

   execution model, on-card cryptography, protecting against attacks

4. Card Management

   loading-installing-deleting applets, security aspects

Literature

- Specifications

ISO 7816	`www.iso.org`
Sun JavaCard 2.2.1	`java.sun.com/products/javacard/index.jsp`
Global Platform 2.1.1	`www.globalplatform.org`

- Books

Rankl, Effing. ***Handbuch der Chipkarten.*** *Hanser-Verlag, 2002.*

Chen. ***Java Card Technology for Smart Cards.*** *Addison-Wesley, 2000.*

Schneier. ***Applied Cryptography.*** *Wiley & Sons, 1996.*

Menezes et al. ***Handbook of Applied Cryptography.*** *CRC Press, 1996.*