  
innovations  
for high  
performance  
microelectronics

---


**Integrating Mobile Devices into E-business  
Architectures: Open Issues and Potential  
Solutions**

**Dr. Peter Langendörfer**  
**Zoya Dyka, Frank Vater and Prof. Dr. Rolf Kraemer**

**IHP**  
**Im Technologiepark 25**  
**15236 Frankfurt (Oder)**  
**Germany**

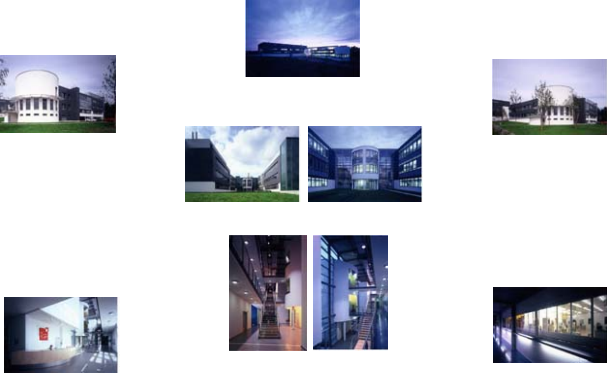
---

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved




**New Institute and Cleanroom**

---



---

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved



## IHP in a Nutshell

---

**The Institute**

- Founded in 1991; successor institution to the former institute of the East German Academy with extensive experience in silicon microelectronics
- 200 employees from 16 countries
- Member of the Gottfried Wilhelm Leibniz Society (WGL)

**Mission**

- Strengthen the competitive position of the German and European microelectronic and communication research
- Act as an innovation center, leading research results towards prototypes
- Enhance the attractiveness of the region as location for high technology

**Facilities**

- Complete innovation chain from materials to systems, including class-1 c.leanroom, 0.13  $\mu\text{m}$  capable pilotline

**Competencies**


- Systems for wireless communication
- RF circuit design
- Extension of silicon CMOS technologies
- Materials for microelectronic technology

**Strategy**

- Create value through innovation
- Focus on solutions for wireless & broadband communications
- Development of forward-looking technologies and system-level prototypes
- Strategic partnerships

---

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany[www.ihp-microelectronics.com](http://www.ihp-microelectronics.com)© 2005 - All rights reserved



## Outline

---

- **Motivation**
- **Communication Protection Means**
- **Application of Crypto Means**
- **Energy Issues**
- **Challenges Ahead**

---

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany[www.ihp-microelectronics.com](http://www.ihp-microelectronics.com)© 2005 - All rights reserved

### Motivation: B2C



- Privacy ranked issue the # 1 Internet issue for consumers (Business Week survey 1998)
- 87% of experienced Internet users concerned about online privacy invasion (AT&T survey 1999)
- 59% want more federal privacy legislation (Business Week survey 2001)
- USD 15 billion could be lost by online retailers in 2001 because of consumers privacy concerns (Forrester research 2001)
- 34% of Internet users would start purchasing from online retailers if privacy was guaranteed (Forrester research 2001)
- 27% abandoned online purchases because of privacy concerns (Cyber Dialog survey 2001)

### Location-aware applications

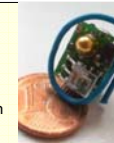


- Location aware mall – Metro Future-Store  
Location aware shopping system  
Finds location of products





- Ubiquitous Mall  
Mobile communication + sensors/RFID tags

Sensor node  
• tiny 1cm<sup>3</sup>  
• sensors,  
• battery,  
• CPU,  
• communication  
Source: www.teco.edu





Registers what you buy???




### Location-awareness and privacy

  • Advertisement for new violin received on handheld  
• No personal information provided

+

  • Tobacco for pipe bought; paid using handheld  
• No personal information provided

+

 Bakerstreet  • Bus taken to go home  
• Handheld is still running = 

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany www.ihp-microelectronics.com © 2005 - All rights reserved

### Privacy Risks

- **Spamming**
- **Profiling (Value of a profile 15-50 € [ Source: F-Secure])**
- **Physical location tracking**
- **Identity theft**
- **Surveillance**

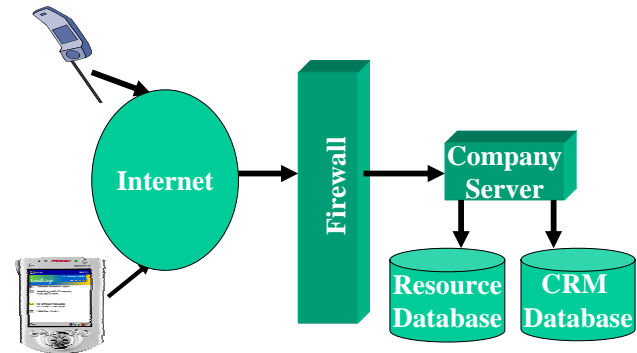
IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany www.ihp-microelectronics.com © 2005 - All rights reserved


### Privacy Protection



- **Do not give away any information**
  - Highly secure
  - No use of online service possible
- **Restrict dissemination of data to the very minimum**
  - Use secure communication channels
  - Use anonymous payment
  - Negotiate about the data to be provided
- **Make sure that information cannot be linked**
  - Use anonymous payment
  - Use set of pseudonyms

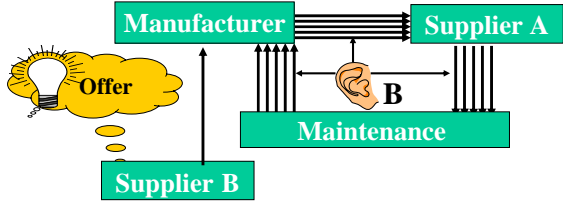
### Business to Employee





**Motivation: B2B & B2E**

- Loss of confidential information
- Loss of image
- Reduced productivity
- Information flow analysis



IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved



**Communication Protection Means**

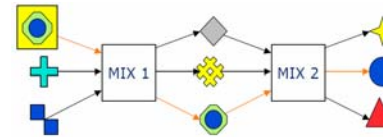
IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved

**Cryptography: THE KEY enabler for Secure Communication**



- **Public key cryptography:**  
provides means to realize: Digital signatures, Key exchange  
computational burden high
- **Secret key cryptography:**  
provides relatively efficient means to en-/decrypt bulk data transfer.  
computational burden low
- **Anonymous communication:**  
protection against message flow analysis: crowds, onion routing  
and mix nets  
computational burden very high

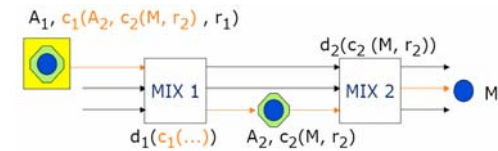
**Mix Net Approach**




- Send packets in a burst, not continuously
- Packets have the same size
- At least one mix is not attacking

**Public Key Cryptography**

- $c_i(\dots)$  public key of mix<sub>i</sub>
- $d_i(\dots)$  private key of mix<sub>i</sub>
- $A_i$  address of mix<sub>i</sub>
- $r_i$  random number
- $M$  messages including address of final destination



Source: Prof. H. Federrath Uni Regensburg




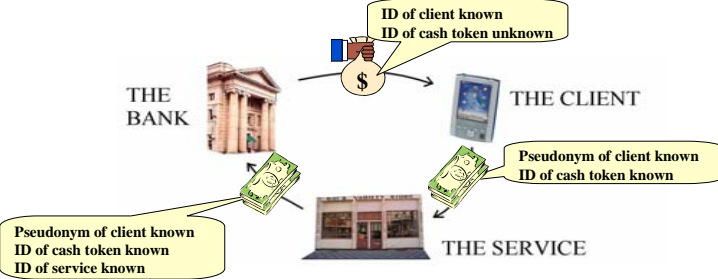
---

## Application of Crypto Means

---

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved

**Moneta: An anonymous payment scheme** 



The diagram illustrates the Moneta payment scheme. It shows three main entities: THE BANK, THE CLIENT, and THE SERVICE. THE BANK provides money (represented by a dollar sign) to THE CLIENT. THE CLIENT then uses this money to pay THE SERVICE. Information flow is indicated by callouts: 1. From THE BANK to THE CLIENT: 'ID of client known', 'ID of cash token unknown'. 2. From THE CLIENT to THE SERVICE: 'Pseudonym of client known', 'ID of cash token known'. 3. From THE SERVICE to THE BANK: 'Pseudonym of client known', 'ID of cash token known', 'ID of service known'.

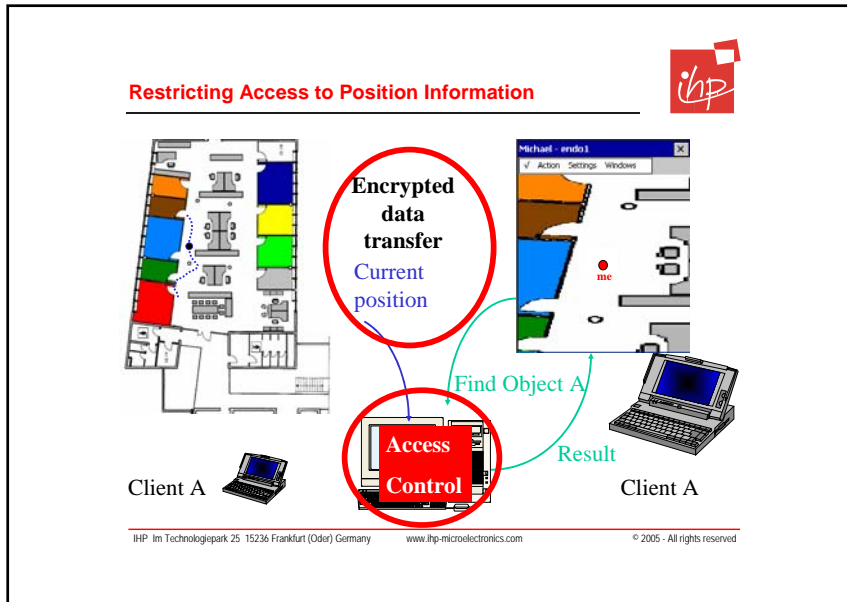
**Hidden Identity Approach requires heavy use of public key cryptography**

**Secure Communication requires heavy use of secret key cryptography**

---

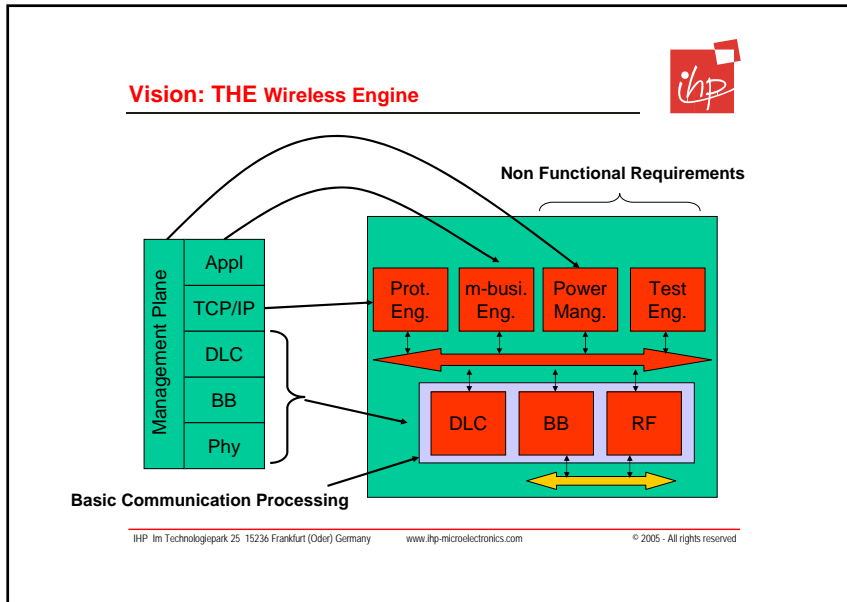
IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved





## Energy Issues

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved



**Energy Consumption**

- Up time of mobile devices is significantly decreased by
  - Wireless communication
  - Cryptographic means

	Total up time in minutes using a WLAN connection		Total up time in minutes w/o wireless communication	
	with ciphering	w/o ciphering	with ciphering	w/o ciphering
Video application	125	142	222	256

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany www.ihp-microelectronics.com © 2005 - All rights reserved

**Crypto Hardware: Reducing the Energy Consumption**



**Performance of Specialized Hardware vs. Software Solutions**

- Three orders of magnitude less in energy consumption
- Two orders of magnitude less in time consumption

Secret Key Cryptography: Simulation Results for 100 Mbit data using AES;

	Clock cycles	Power consumption
Software	5 357 031 250	178500 mWs
Hardware	10 937 500	66 mWs

Public Key Cryptography: Simulation results for a single elliptic curve point multiplication (B233);

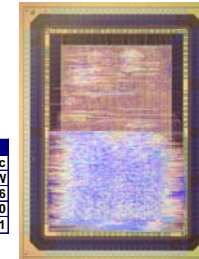
	Clock cycles	Power consumption
Software	14 321 826	478 mWs
Hardware	90 404	0.8 mWs

**Dual<sup>2</sup> Crypto Chip**



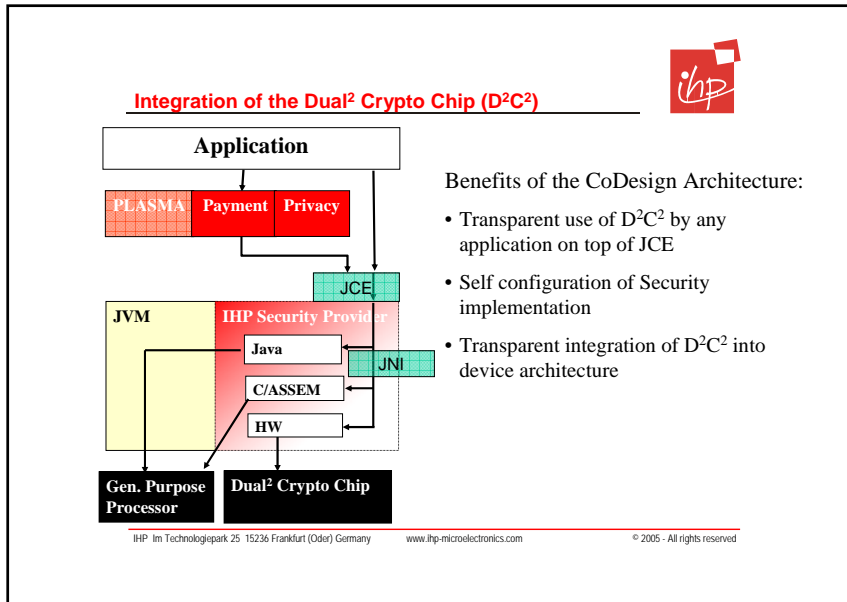
- Dual Crypto Support:
  - Secret Key Cryptography: Advanced Encryption Standard (128bit)
  - Public Key Cryptography: Elliptic Curve Cryptography (233 bit)

- Dual Interface
  - PCMCIA
  - Cardbus





- Characteristics


	AES (128bit)	ECC (233bit)
Throughput @33Mhz	42Mbit/sec	0.85 Mbit/sec
Power consumption @33Mhz	9.59 mW	56.85mW
Complexity KGates	14.44	27.26
Rate (clock cycles)	100	9000
Size (mm <sup>2</sup> @ .25µ Technology)	1.01 mm <sup>2</sup>	2.11





- ### Conclusions & Research Challenges Ahead
- **Current situation**
    - Technical means to protect communication are available
    - BUT:** data given away still cannot be controlled
    - BUT:** High security level and long up times are still contradicting
  - **Sensor Networks & RFID technology are worsening the situation**
    - Direct recording of data (sensor measuring parameters of the user)
    - Indirect recording e.g. groceries are tagged and gather data
  - **Open issues**
    - Management of security setting of mobile devices
    - Firewall protection on the mobile device
- IHP - Im Technologiepark 25 15236 Frankfurt (Oder) Germany    www.ihp-microelectronics.com    © 2005 - All rights reserved


**If everything works fine:** 

 • Advertisement for new violin received on handheld  
• No personal information provided

 **Access to location information denied**

 • Tobacco for pipe bought; paid using handheld  
• No personal information provided

 **Access to location information denied**

 • Bus taken to go home = ?  
• Handheld is still running

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany www.ihp-microelectronics.com © 2005 - All rights reserved



---

**Thank you for your attention!**

**Questions or Comments?**

**Acknowledgements**  
This work was partially supported by the bmb+f (ministry of education and research) under grant 01AK060B.

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany www.ihp-microelectronics.com © 2005 - All rights reserved