Implementing high-level Counterfeit Security using RFID and PKI

Drugs as example products

“RFID SysTech 2007” June, 13

Andreas Wallstabe, Hartmut Pohl

Fachhochschule Bonn-Rhein-Sieg

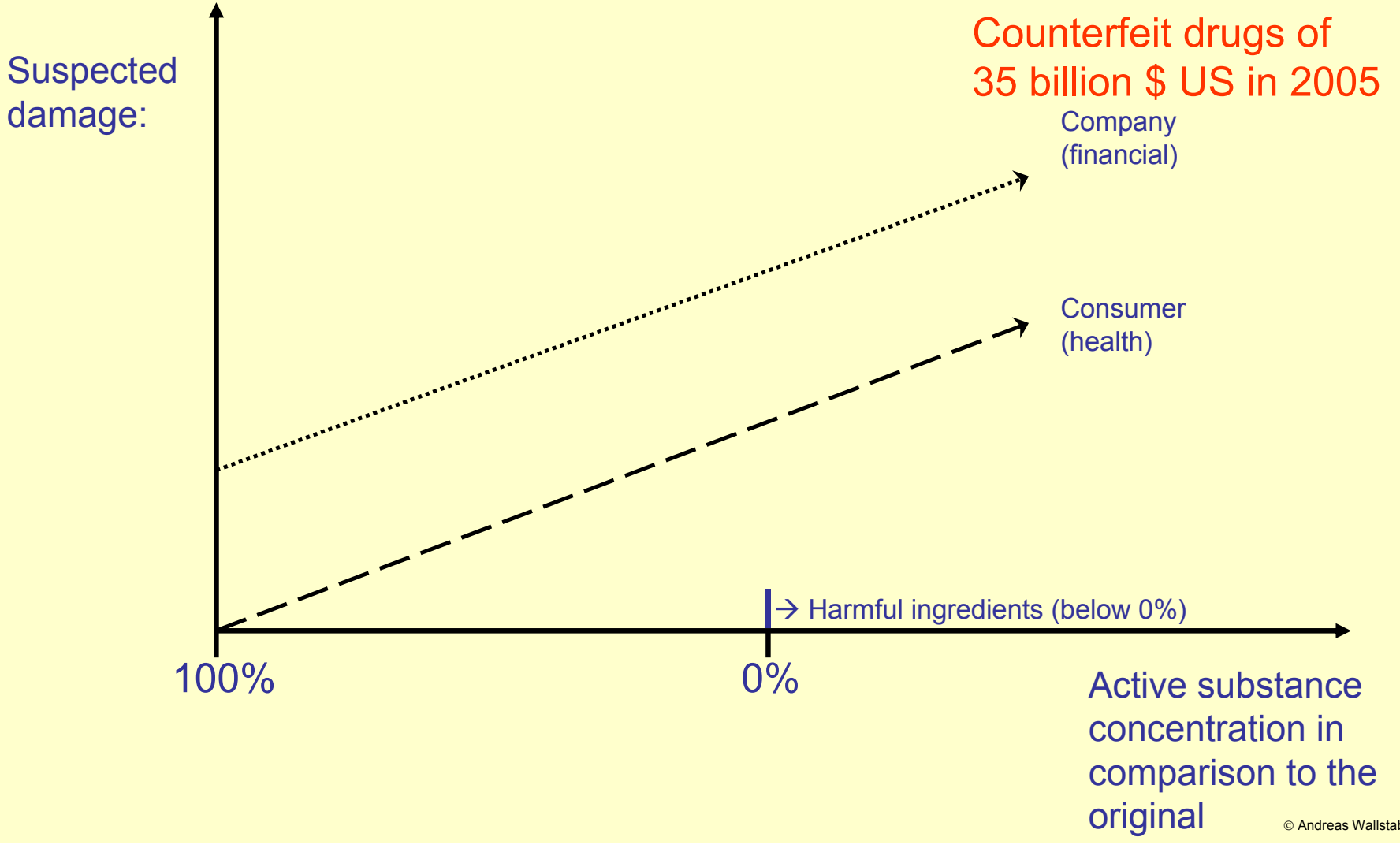
Implementing high-level Counterfeit Security

- Counterfeit Security
- Technologies RFID, PKI
- Anti-Counterfeiting by RFID and PKI
- Implementation, Hardware configuration
- Review und Future

Implementing high-level Counterfeit Security

- Counterfeit Security
- Technology RFID / PKI
- Anti-Counterfeit by RFID and PKI
- Implementation/ Hardware configuration
- Review and Future

Damage estimation of counterfeit drugs



Implementing high-level Counterfeit Security

Counterfeit security

- Validation of an supposed identity by special features
- The counterfeiting effort must be worth more than the feasible benefit and profit of the counterfeiter
  → Counterfeit secure
- Benefit/Profit:
  - Financial
  - Authority, Respect
  - Damage against other
- There is no 100% security

Implementing high-level Counterfeit Security

Counterfeit Security

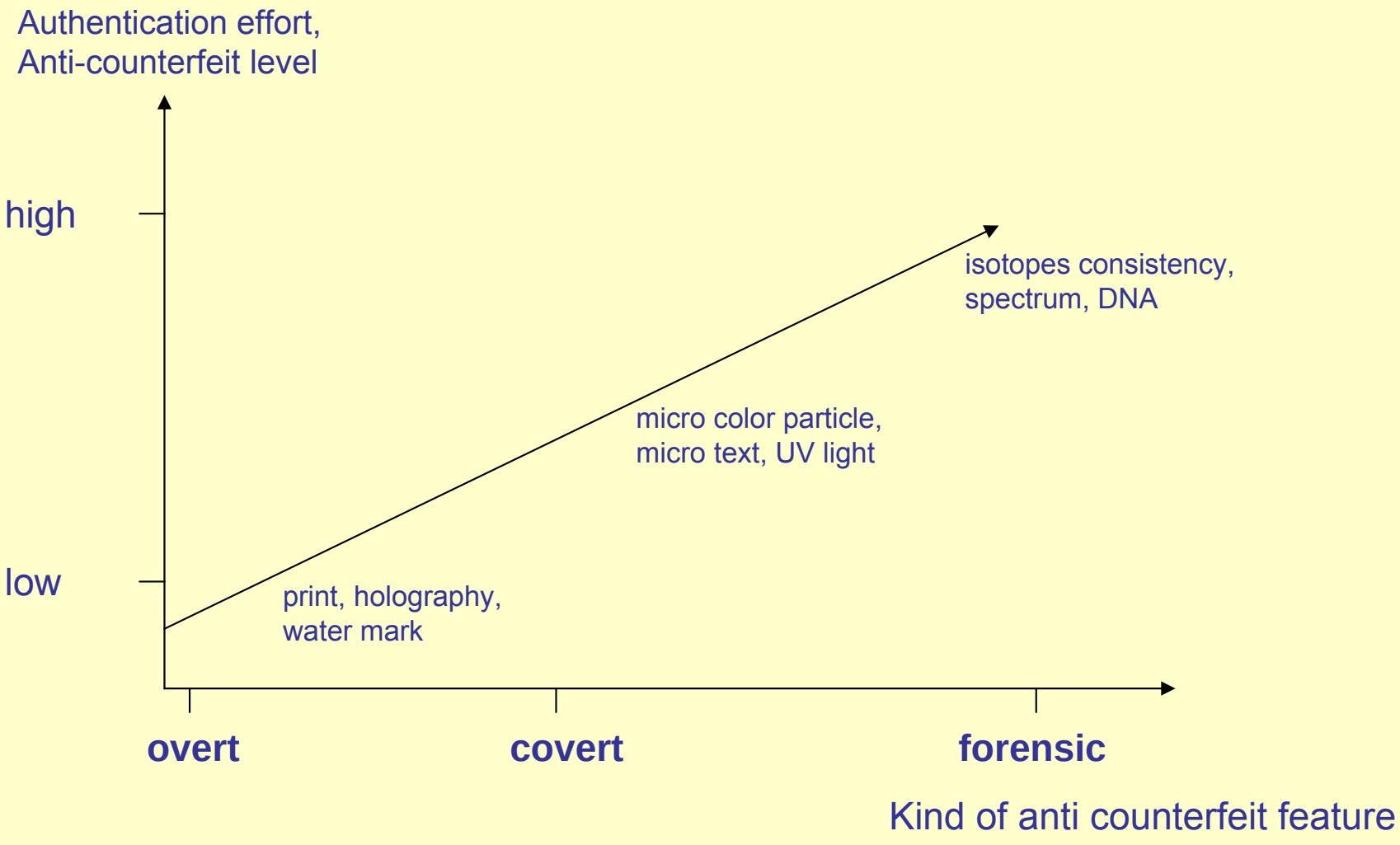
Technology RFID / PKI

Anti-Counterfeit by RFID and PKI

Implementation/ Hardware configuration

Review and Future

Counterfeit security rating



Implementing high-level Counterfeit Security

RFID Radio Frequency Identification

- Physical security
  - Static analysis:
    - Dummy-Structures / Memory usage / Protection layers / Scrambling
  - Dynamic analysis:
    - Passive monitoring / Voltage monitoring/
    - Frequency monitoring / Different kinds of memory
- Software security
  - Test routines for hard- and software/ Checksums/
  - Encapsulating / Deactivation / General processes

Implementing high-level Counterfeit Security

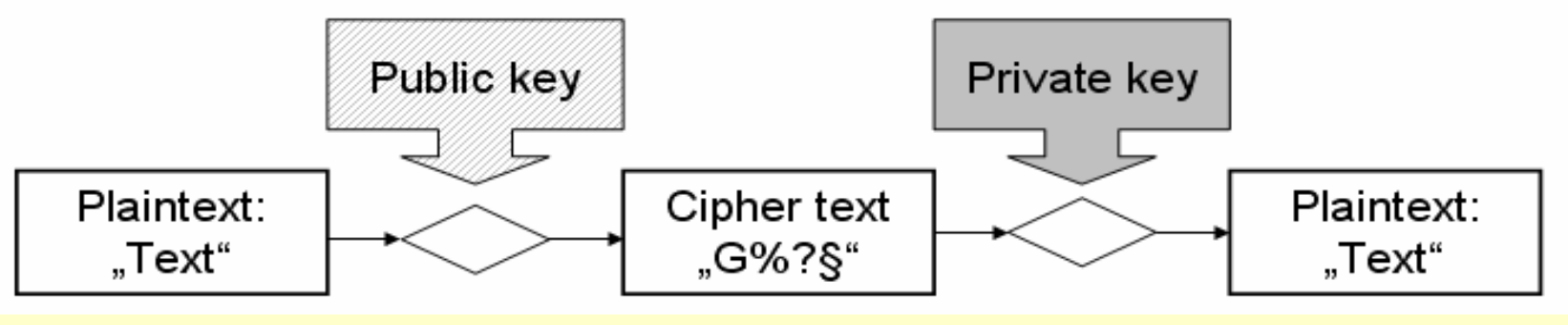
RFID Radio Frequency Identification

- Security aspects
  - + considered: Transponder, Data transmission to the reader device
  - – not considered: Reader device, System development, Production, Application, Social aspects

Implementing high-level Counterfeit Security

PKI Public Key Infrastructure

- Public Key Infrastructure
  - public verifiable (for everybody)
- Asymmetric encryption



- Digital signature
  - Like a signature by hand (Germany 2001)
  - Enables reliability → Authentication

Implementing high-level Counterfeit Security

Counterfeit security by RFID and PKI

- Available technologies
  - TI and VeriSign
  - Patent “product security system”
  - Using transponder as memory
  - Easy to clone
- Intelligent combination
  - Storing the signature on the transponder
  - Transponder becomes an intelligent part of the system
  - Transponder is able to authenticate itself

Implementing high-level Counterfeit Security

Counterfeit security by RFID and PKI

- Security rating of the combination
  - Attacks: Communication/ Key/ Algorithm /Physically

- Resistance of RSA

  (has to be verified continuously)

Bit	MIPS- years to factorize	Cost to break the resist value in two years
512	3000	1500 Euro
768	$2*10^8$	10 million Euro
1024	$3*10^{11}$	15 billion Euro

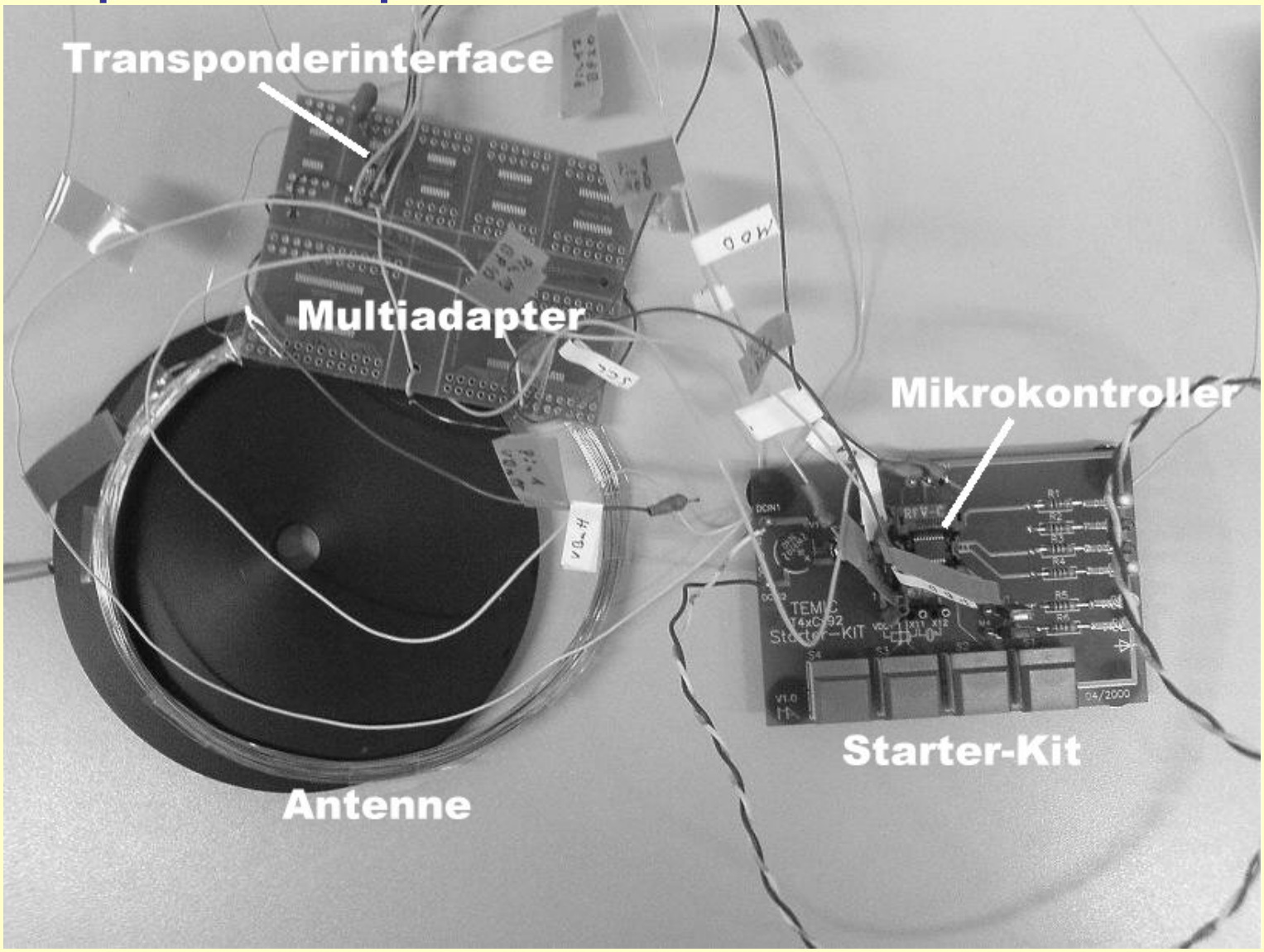
Implementing high-level Counterfeit Security

Hardware

- Microcontroller ATAM893
  - 4-Bit, 4-KByte ROM, Current consumption 20µA
- Transponderinterface U3280M
  - Contact less communication, Power supply
- Connection of components
  - Adapter, Antenna, Capacitor, Starter-Kit T4xCx92

Implementing high-level Counterfeit Security

Transponder Components



Implementing high-level Counterfeit Security

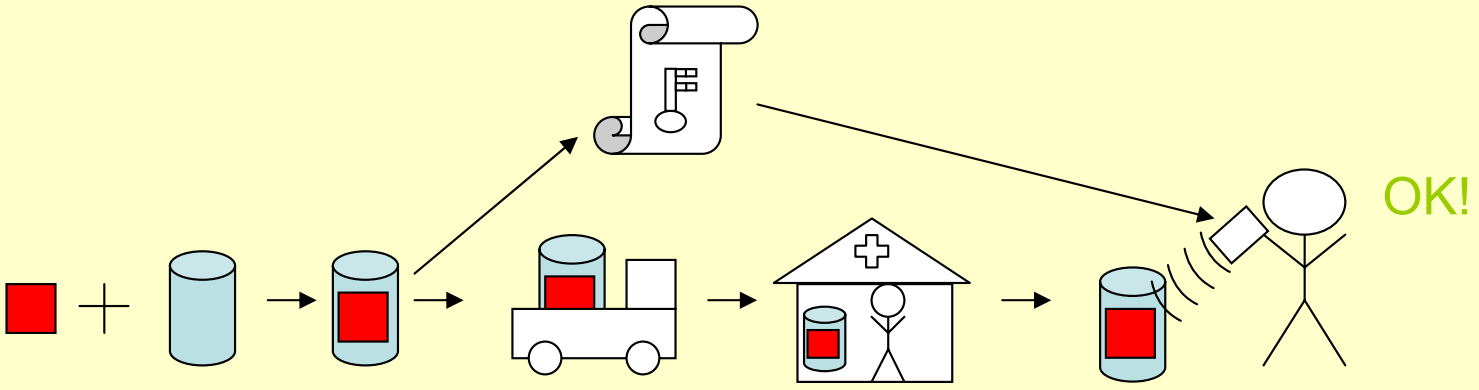
Software

- qForth and MARC 4 are stack oriented
- 4-Bit Microcontroller, no libraries for multiplication with overflow, Modulo, Encryption
- Rare resources, proper signature generation
- RSA algorithm for a 8-Bit signature / key realized
- Program sequence
  - Receiving challenge / Signature generation (RSA) / Send response

Implementing high-level Counterfeit Security

Use Case Example

- Transponder with RSA algorithm and private key is attached to a drug
- The public key is distributed in a public directory
- Drug is sold in a pharmacy store
- Customer can proof identity (authentication) on a terminal or at home with the help of the public key
- Check is possible for everybody without knowing any password



Implementing high-level Counterfeit Security

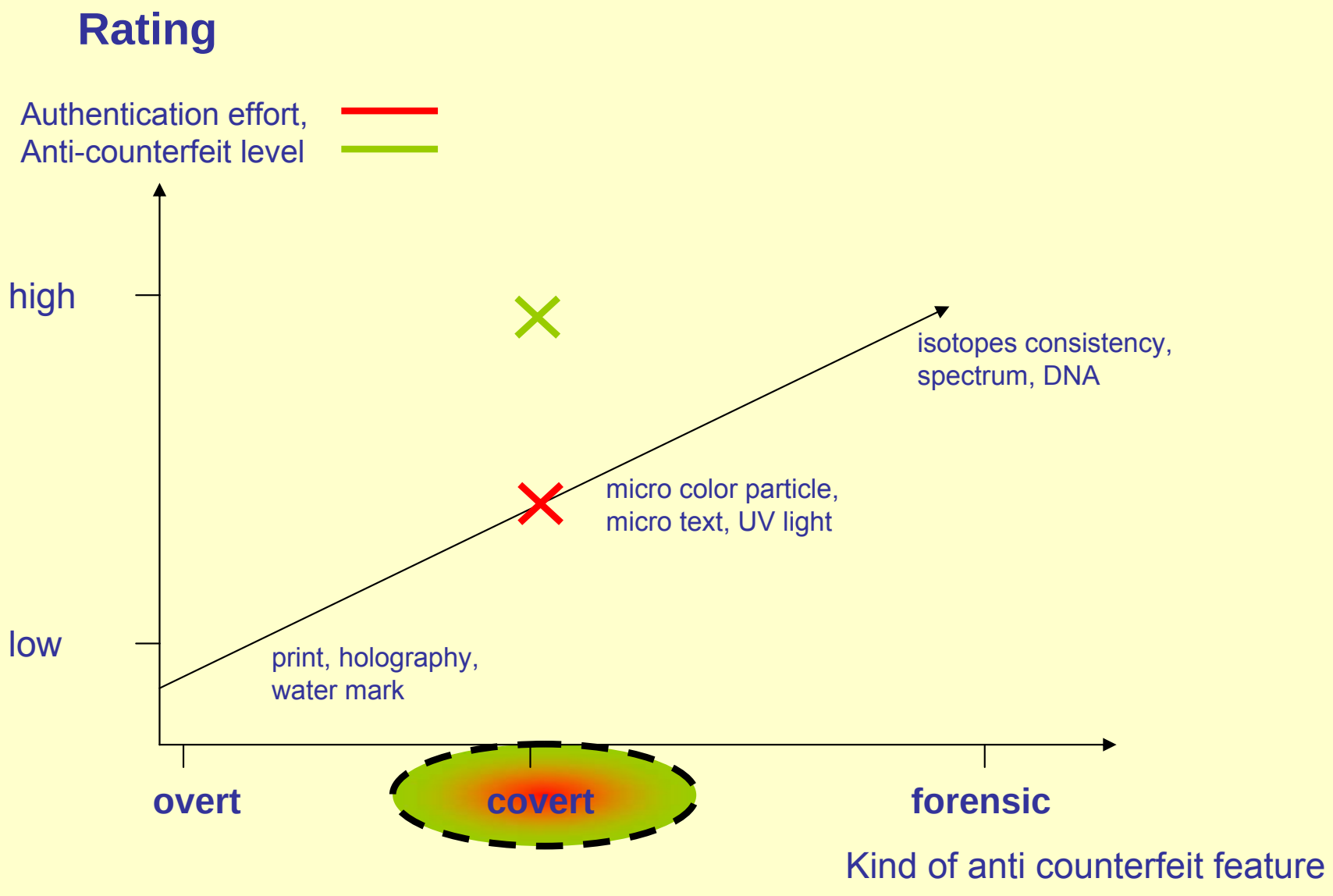
Counterfeit Security

Technology RFID / PKI

Anti-Counterfeit by RFID and PKI

Implementation/ Hardware configuration

Review and Future



Implementing high-level Counterfeit Security

RFID security level

	Process (Security level: 1=low / 6=high)	
6	Public Key Infrastructure, digital signature	Authentication
5	Encrypted communication	
4	Encrypted stored information: program and data	
3	Password protected ID	Identification
2	ID: Object Name Service (ONS)	
1	Unique Identification (UID)	

Implementing high-level Counterfeit Security

RFID security level

	Process (Security level: 1=low / 6=high)	
6	Public Key Infrastructure, digital signature	Authentication
5	Encrypted communication	Authentication
4	Encrypted stored information: prog. data	Authentication
3	Password protected ID	Identification
2	ID: Object Name Service (ONS)	Identification
1	Unique Identification (UID)	Identification

Management

Passive

Management

Cloning

Implementing high-level Counterfeit Security

Conclusion

- New kind of method
- Low price per item
- Resources available (max. 128 / 256 Bit)
- Flexible check for every user possible
  - Supplier/ POS/ Drugstore
- High security level
  (The allocation is one to one)
- Implementation within the next 5 - 10 years

Implementing high-level Counterfeit Security

Thank you for attention

Andreas Wallstabe andreas.wallstabe(at)smail.inf.fh-bonn-rhein-sieg.de
Hartmut Pohl hartmut.pohl(at)fh-bonn-rhein-sieg.de