From (I)MD to Cloud!

Ahmad-Reza Sadeghi, Thomas Schneider, Christian Wachsmann
Fraunhofer SIT Darmstadt and
Technische Universität Darmstadt (CASED), Germany

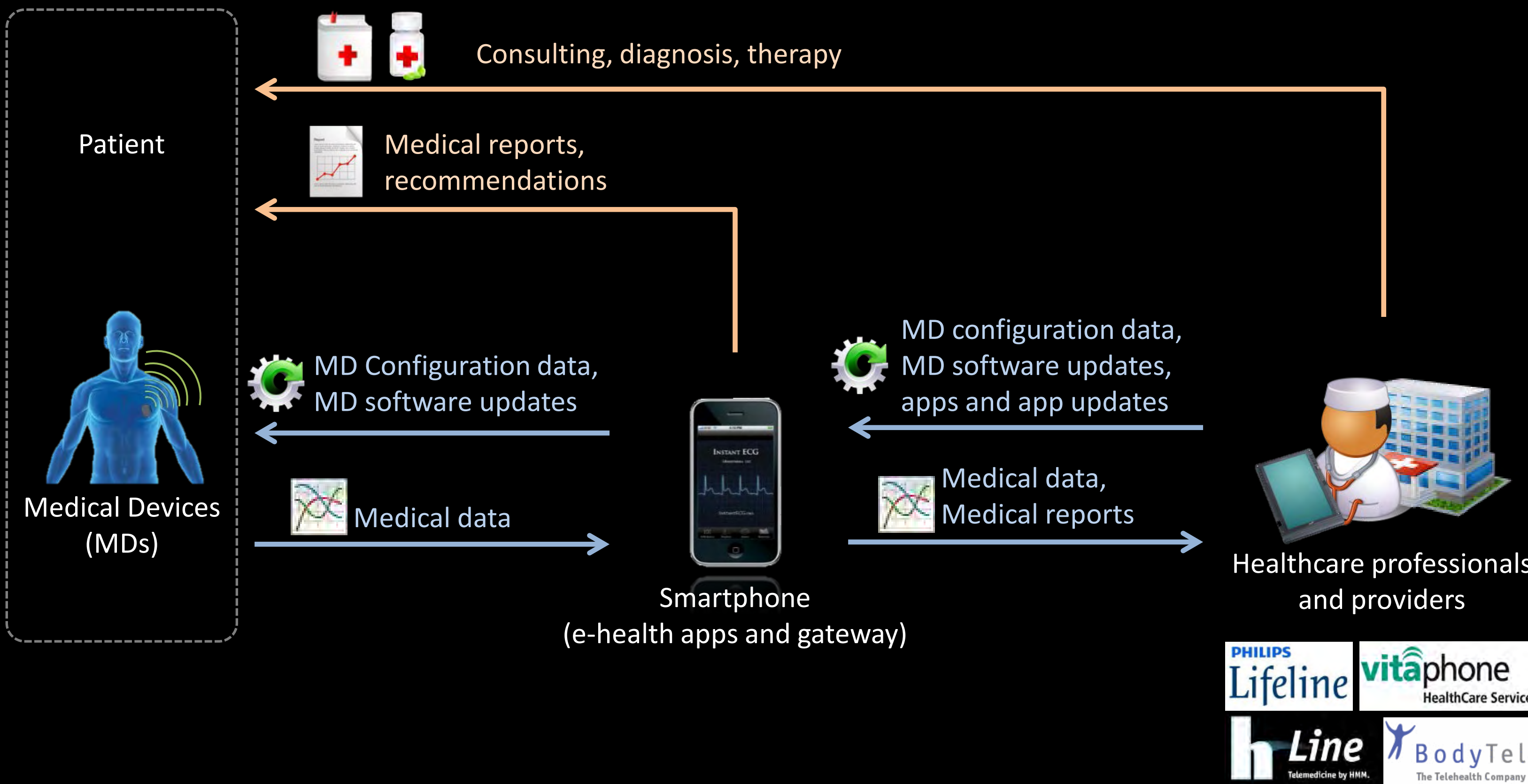
Mina Deng
Philips Research Eindhoven, Netherlands

System Security Lab · Fraunhofer SIT · Technische Universität Darmstadt · CASED

What is a Cool (I)MD ?

Today: Mobile Health Monitoring

Typically single providers and closed systems

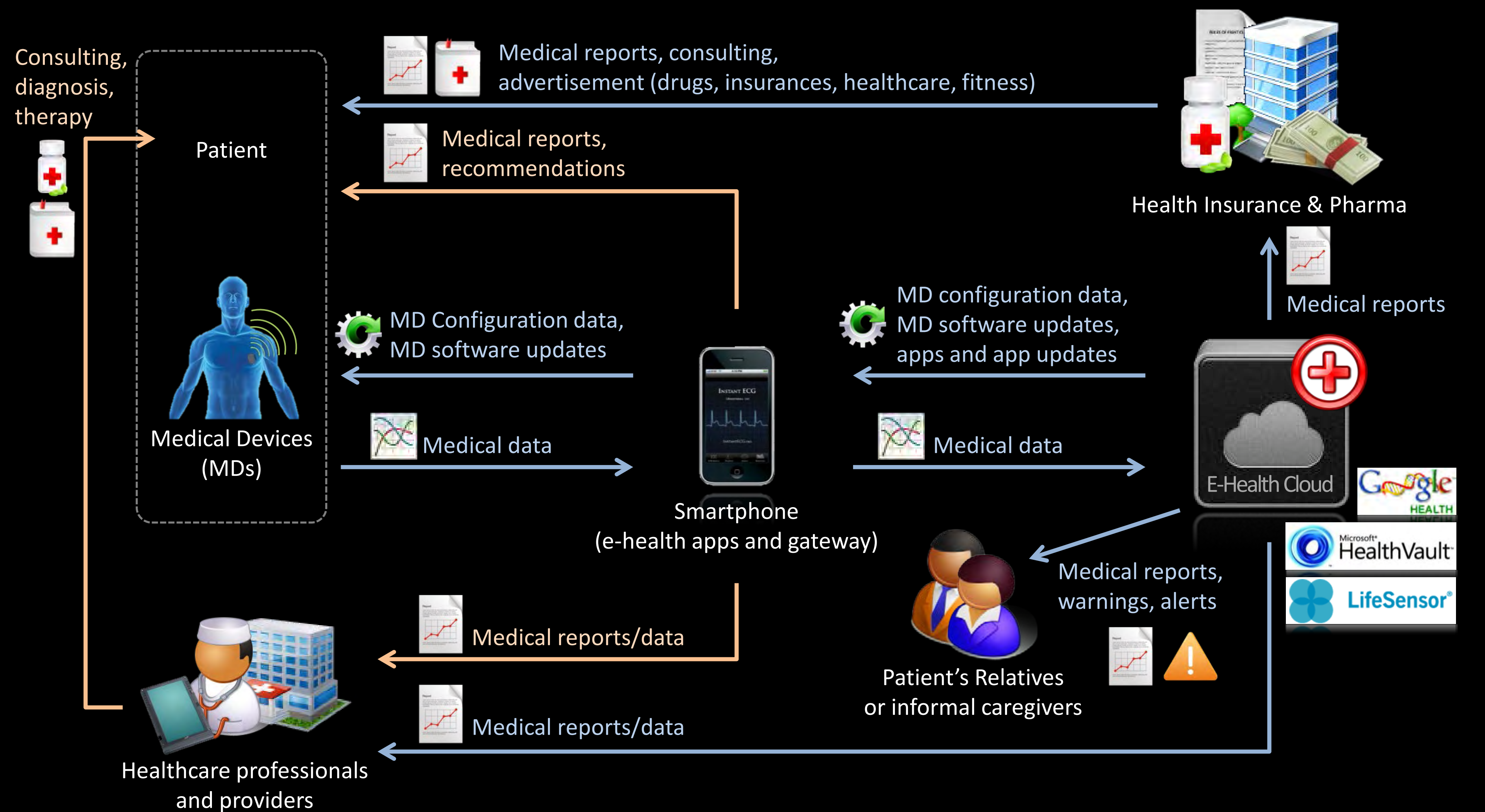


Manually initiated by the patient or doctor

No user interaction, fully automatic

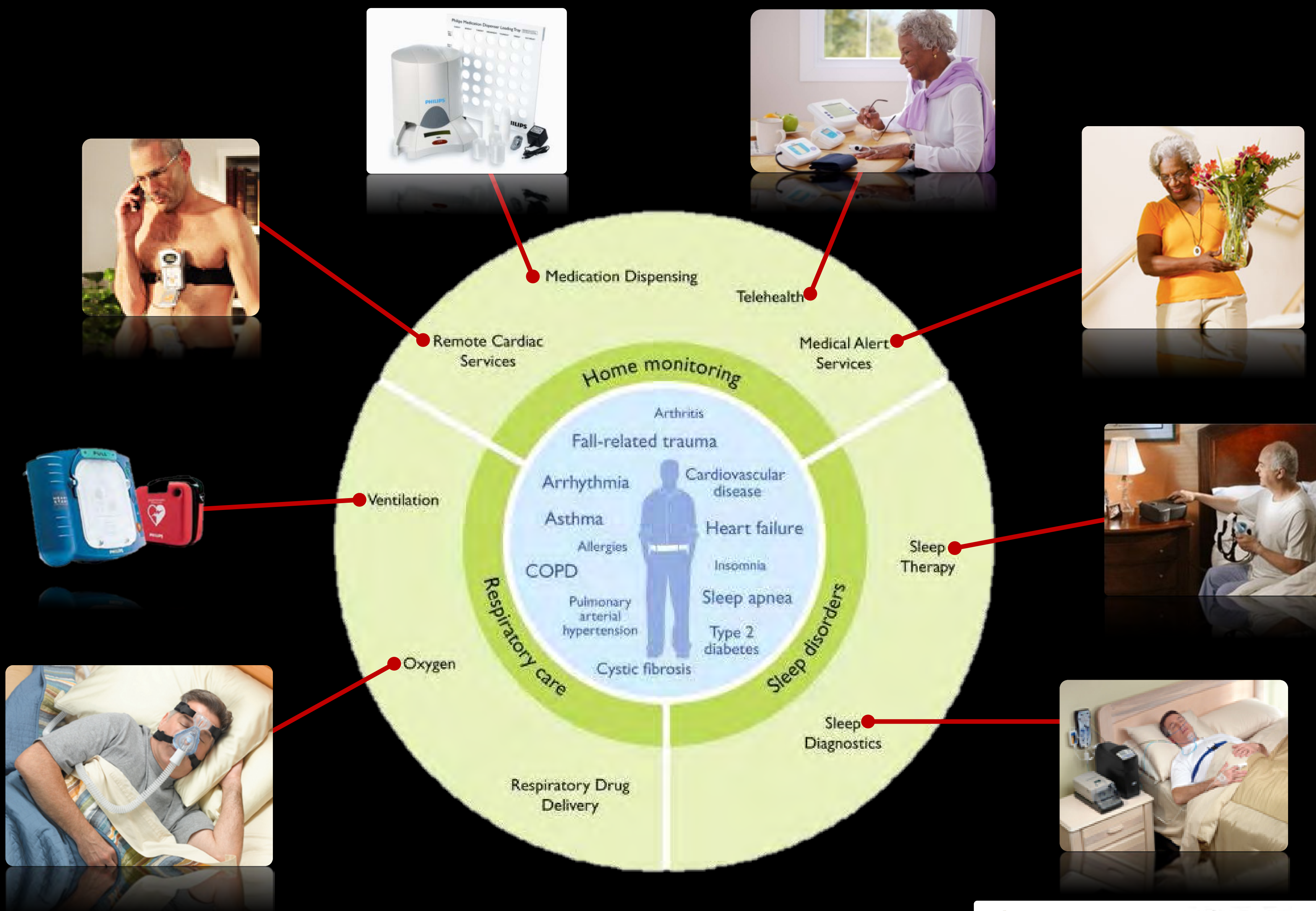
Tomorrow: Mobile Healthcare Network

Different providers and distributed systems



Manually initiated by the patient or doctor   No user interaction, fully automatic

Example: Philips Home Healthcare



Objectives and Challenges

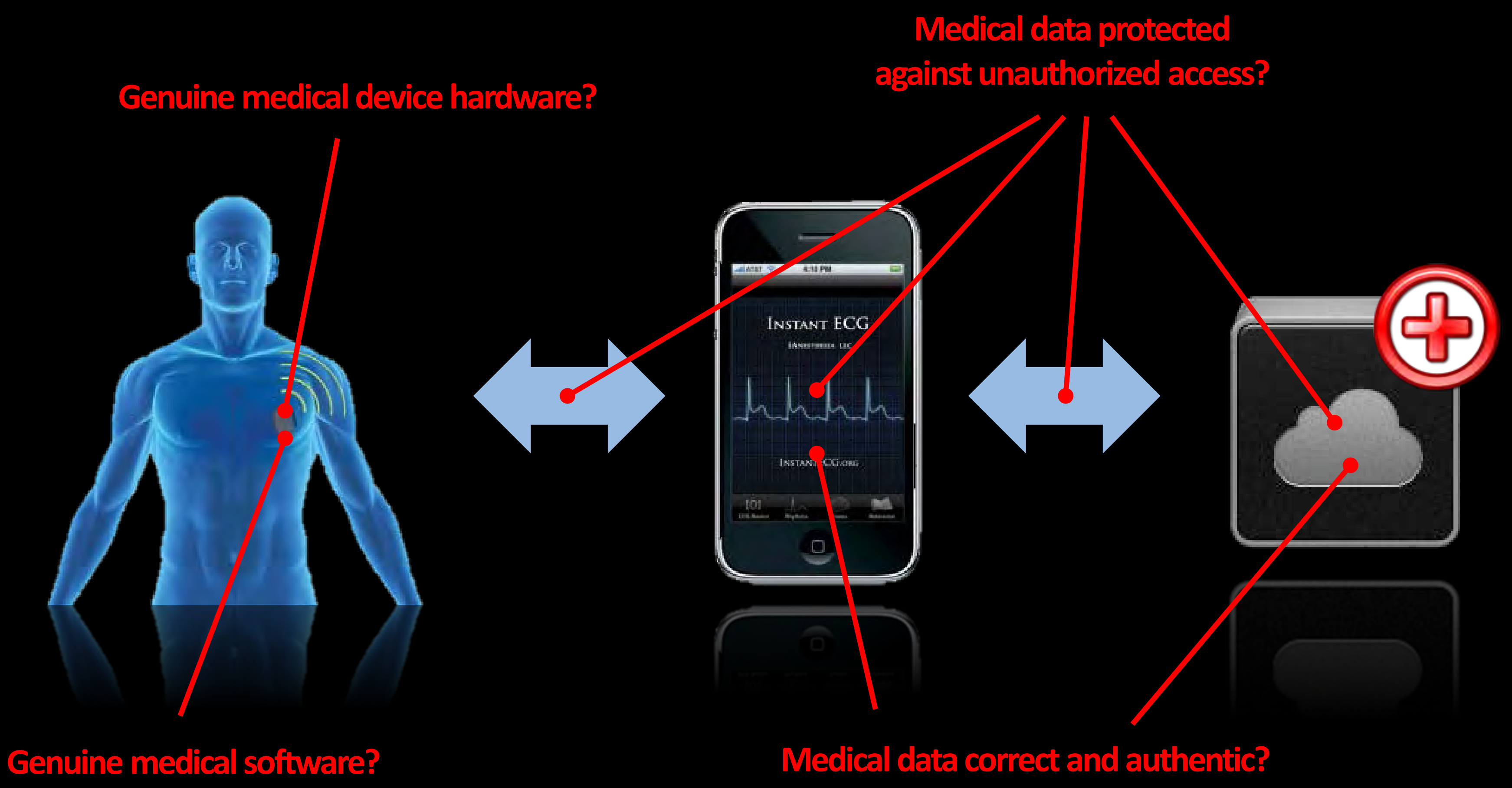
Security

- Data-centric protection
- Semi-trusted cloud service providers (e.g., honest but curious)
- Emergency access and availability
- Reliability, integrity, and confidentiality
- Accountability (incl. integrity of auditing files)
- Efficiency
- Self-management (resilience, availability, adaptability, scalability)

Privacy and Data Protection

- For patients and doctors
- Patient-centric protection and transparency
  (legislation awareness, auditability, policy compliance)

Attack Surfaces



Problems to Tackle

Medical Device Security: Is this device genuine?

- Identification and authentication of medical devices
- Software integrity verification of medical devices

Medical Infrastructure Security: Who, where, when accesses data?

- Mobile Trusted Virtual Domains (TVDs)

Medical Data in the Cloud: Is secure computation possible?

- Privacy-preserving medical classification and diagnosis

Medical Device Security:
Is this device genuine?

unique

www.unique-project.eu

System Security Lab

Fraunhofer SIT

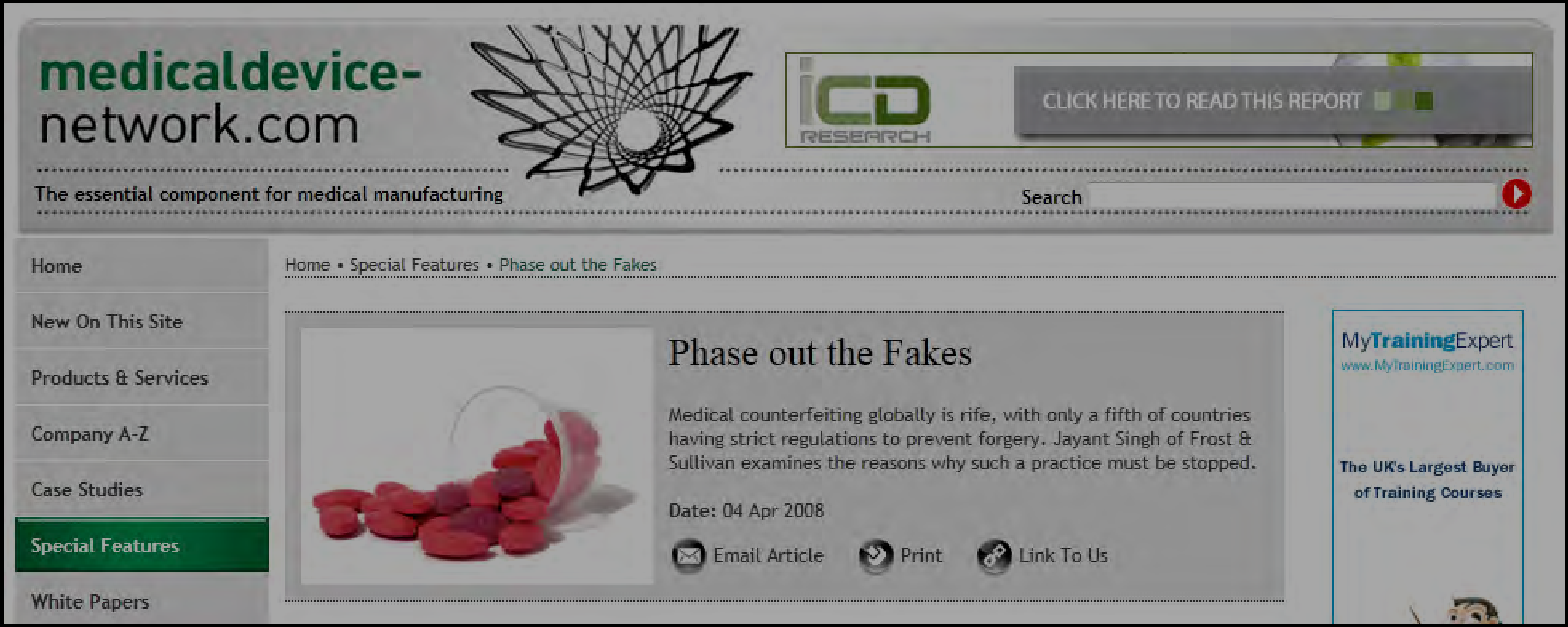
TECHNISCHE UNIVERSITÄT DARMSTADT

CASED

As per an estimate of the OECD and WHO, around 6-8% of the total medical devices market comprises of counterfeit goods.

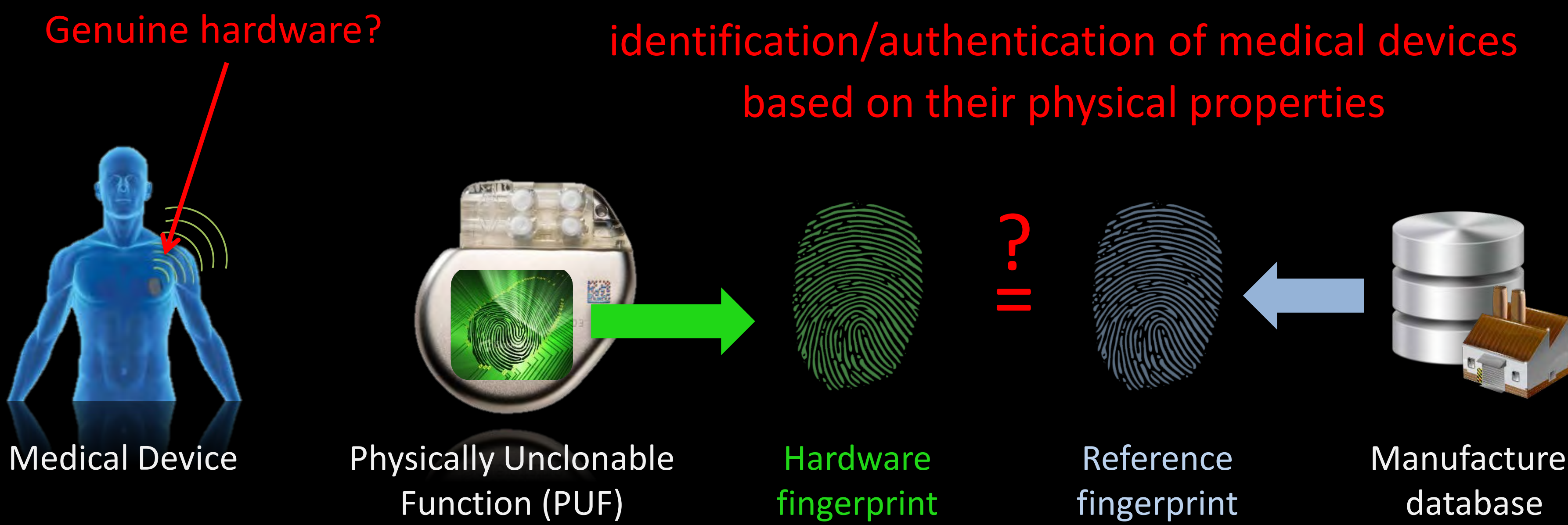
The US FDA reported that intra-aortic pumps worth $7m were recalled after malfunctioning components were found to be counterfeit.

The problem has also attracted the attention of the WHO: more than 2,000 kits containing stethoscopes and sphygmomanometers were seized during transport from China to Greece, and every part of the shipment had been counterfeited - packaging, instructions, devices and European standards marks.



Physical Device Identification

PUFs enable
identification/authentication of medical devices
based on their physical properties



Assumptions

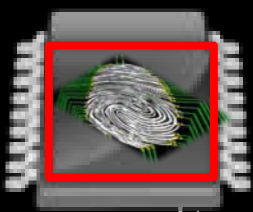
- Adversary cannot predict PUF responses (unpredictability)
- Adversary cannot create physical copy of PUF (physical unclonability)

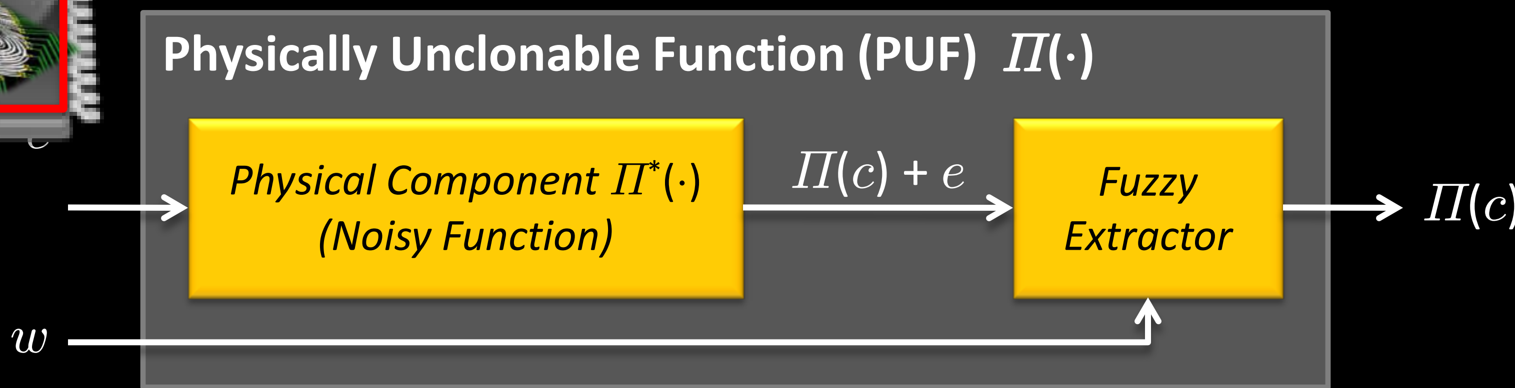
Drawbacks

- Number of authentications limited by size of database
- Inefficient system initialization
- Direct access to PUF may allow modeling attacks

System Security Lab Fraunhofer SIT TECHNISCHE UNIVERSITÄT DARMSTADT CASED

Physically Uclonable Functions





c Challenge

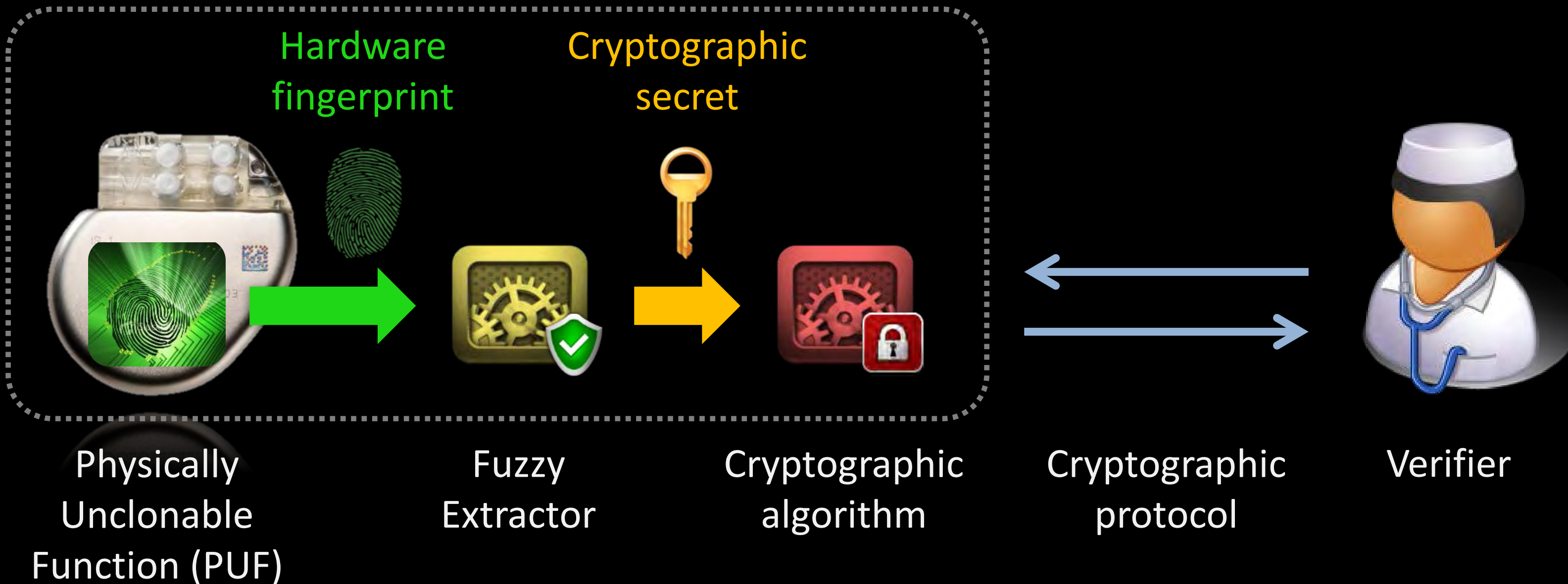
e Error (noise) of Π^*

w Helper data

(to counter noise e, specific for each challenge c)

PUF-based Key Storage

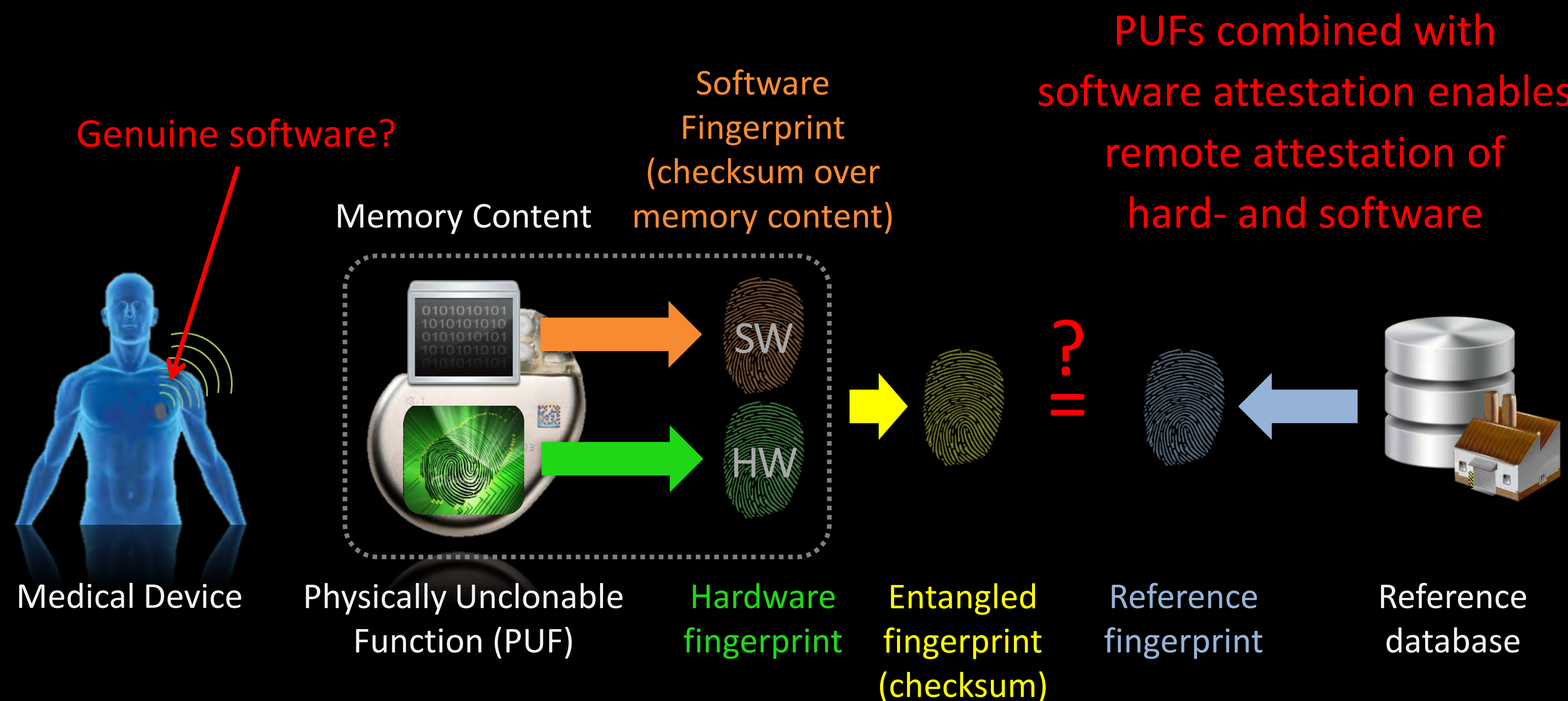
[Šcoric et al. 05, Lim et al. 05]



Assumptions

- Adversary cannot create physical copy of PUF (unclonability)
- Adversary cannot access communication interface between PUF, fuzzy extractor and crypto algorithm

Software Integrity Verification



Assumptions

- Verifier knows exact hard- and software configuration of medical device
- Adversary cannot predict PUF responses (unpredictability)
- Adversary cannot create physical copy of PUF (physical unclonability)

A.-R. Sadeghi, S. Schulz, C. Wachsmann: Lightweight Remote Attestation using Physical Functions. ACM WiSec'11.

Medical Infrastructure Security: Who, when, where access data?

TClouds

www.tclouds-project.eu

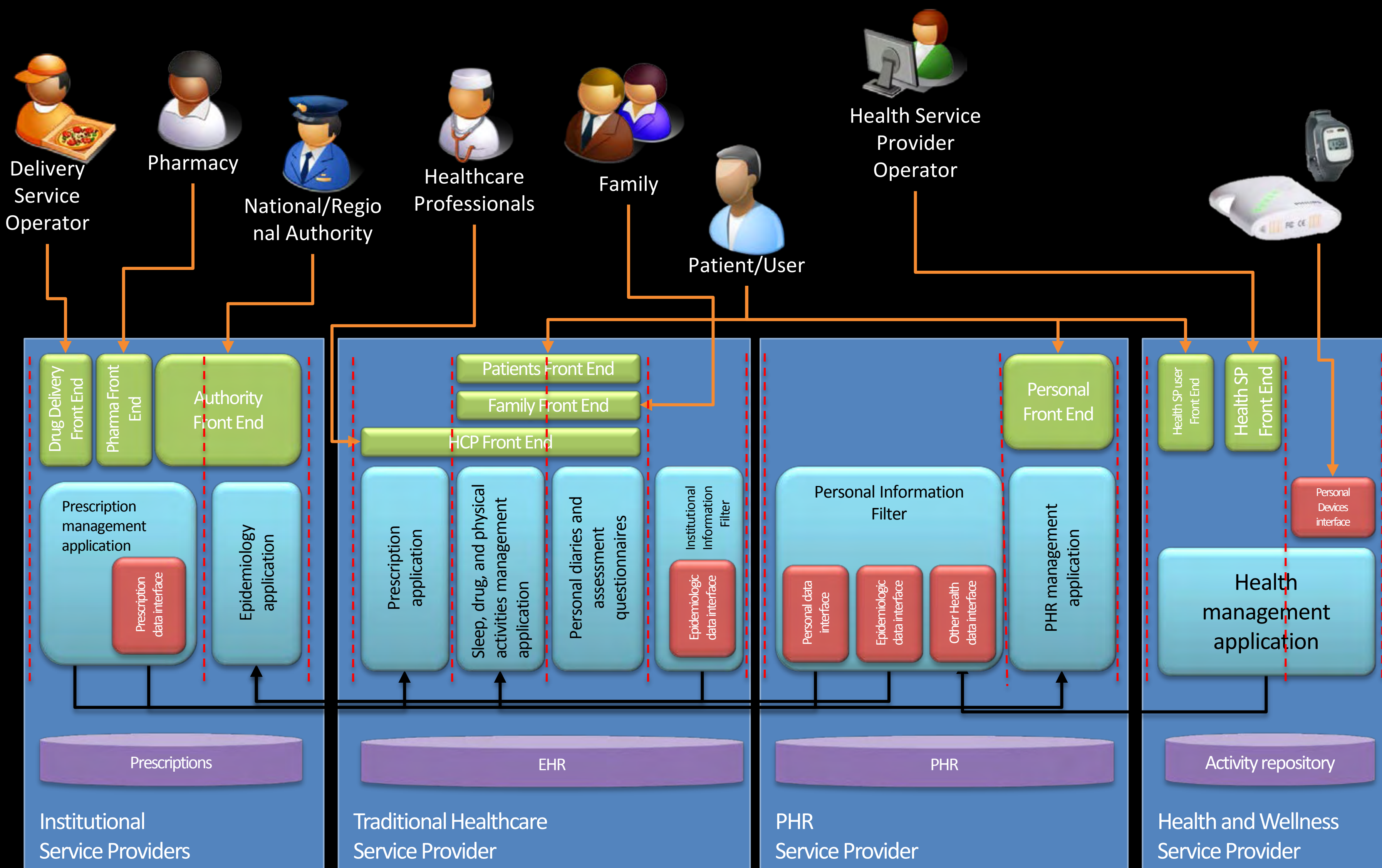
System Security Lab

Fraunhofer SIT

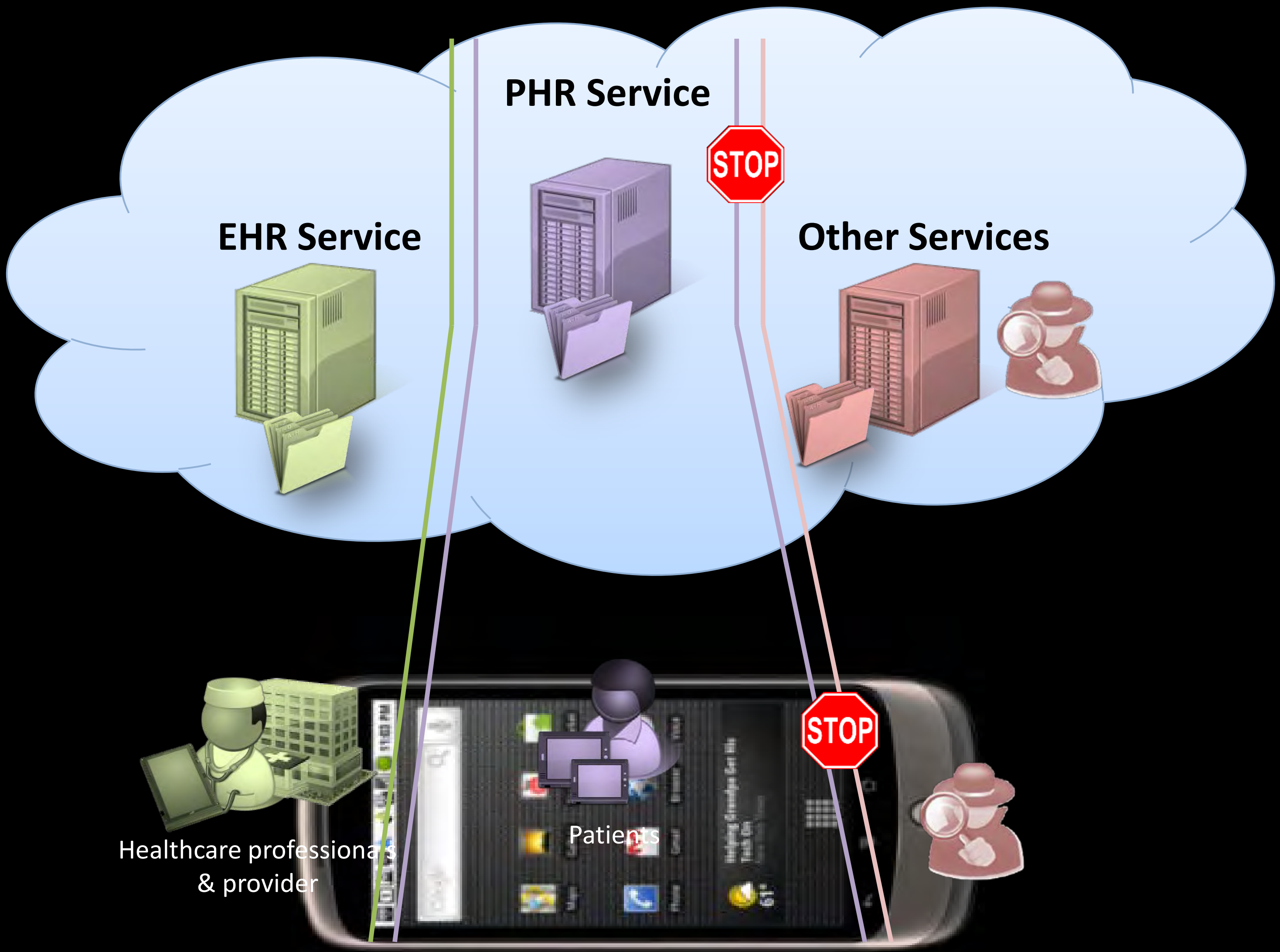
TECHNISCHE UNIVERSITÄT DARMSTADT

CASED

Conceptual Architecture: Global View



Privacy Domains

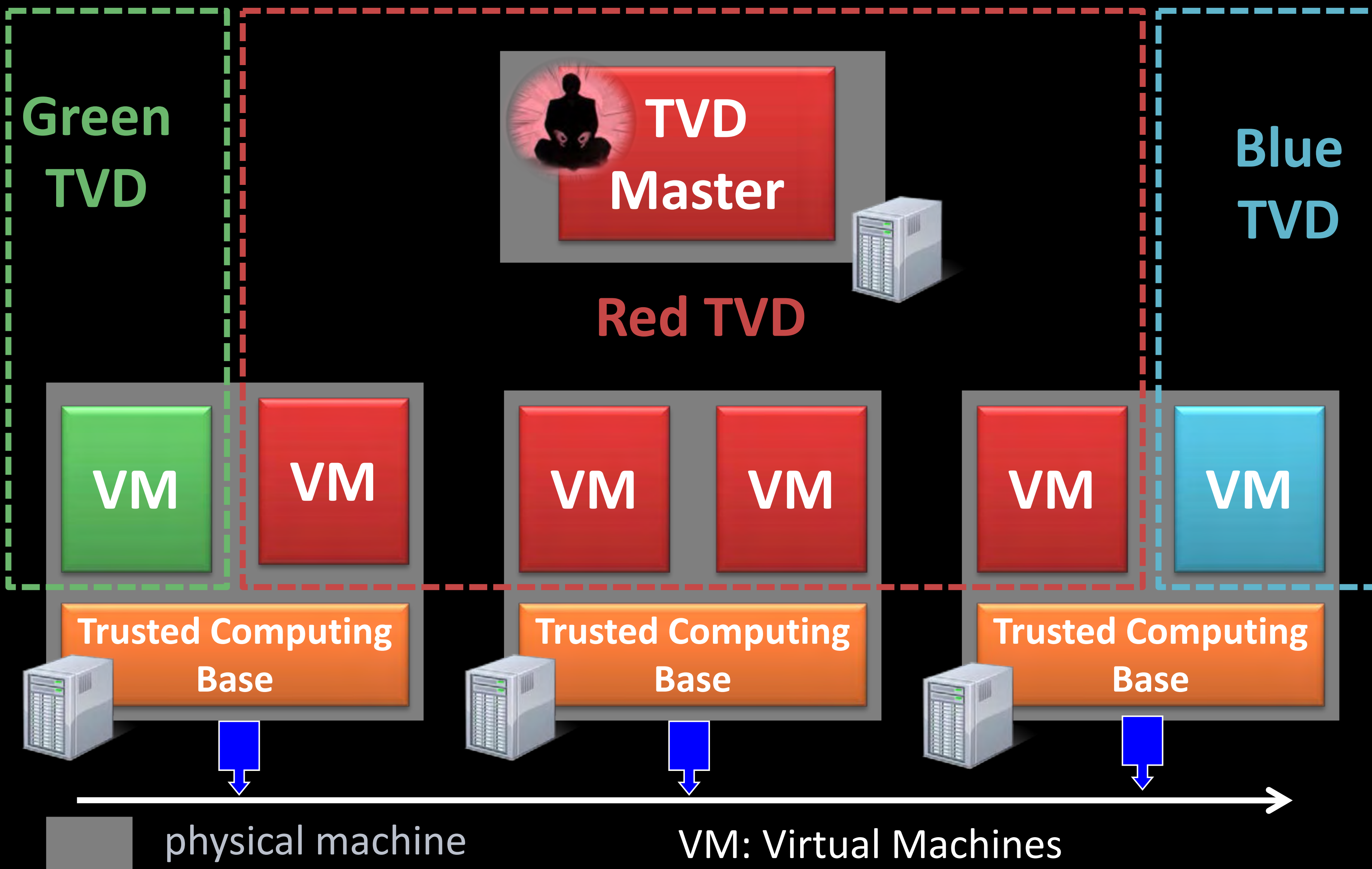


H. Löhr, A.-R. Sadeghi, M. Winandy: Securing the E-Health Cloud. IHI 2010.

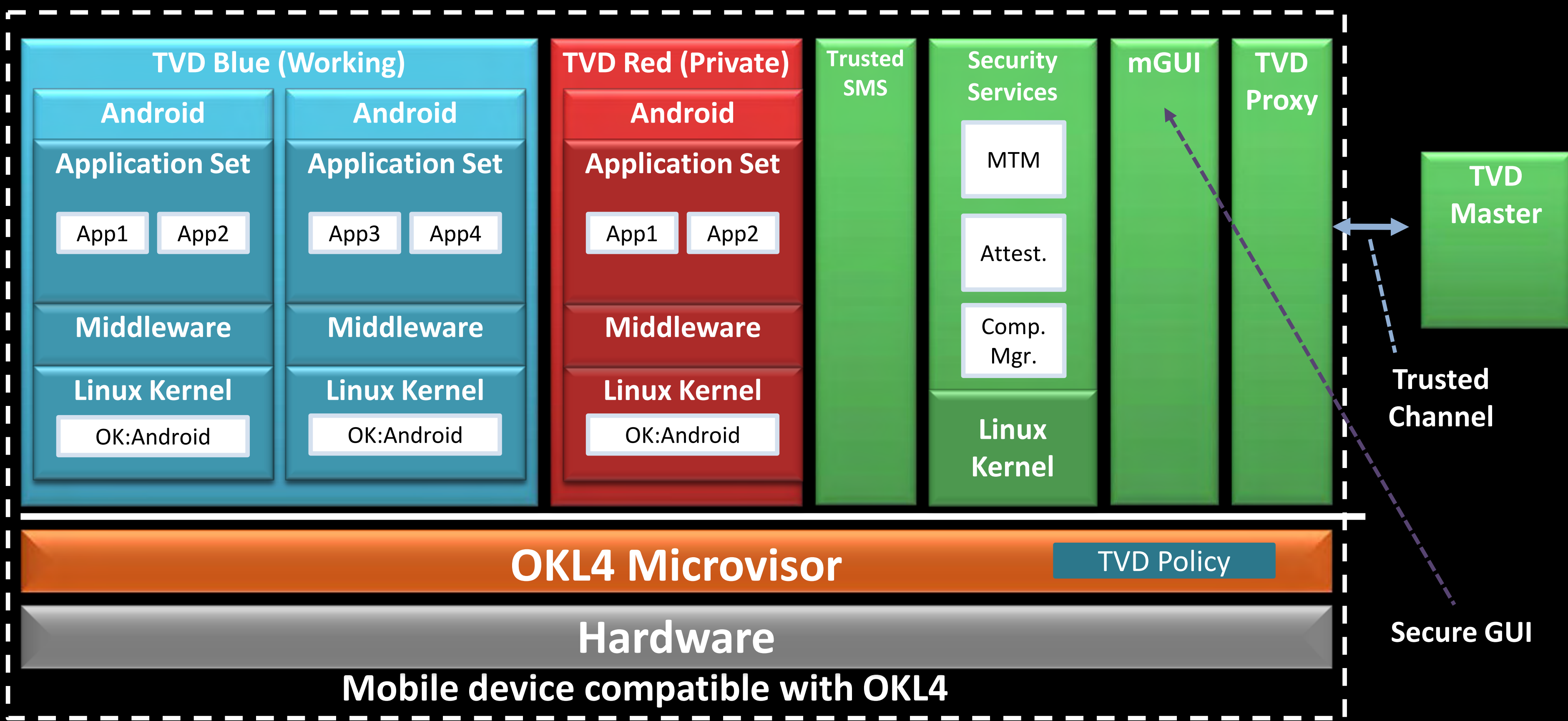
Technology: Trusted Virtual Domains (TVDs)

- **TVD = Coalition of virtual machines**
- **Properties**
  - Isolated execution environments (compartments)
  - Trust relationships
  - Transparent policy enforcement
  - Secure communication
  - Client platform security (based on modern hardware security functionality)

Logical TVD Architecture



Integration of TVD Main Components



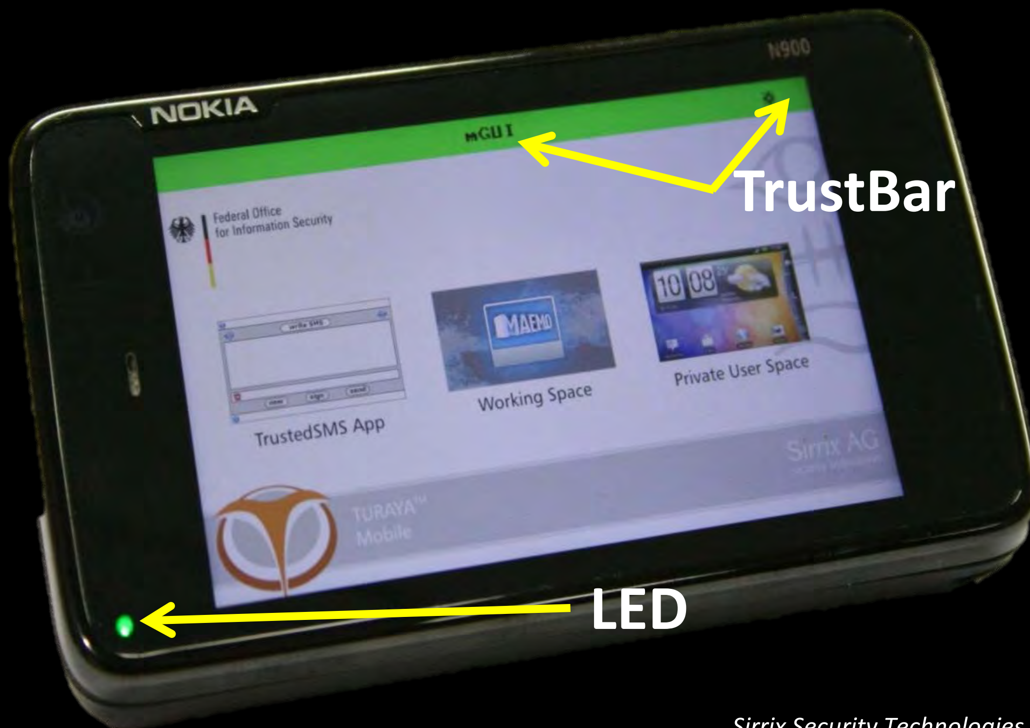
Pro and Contra

- **Pro:**
  - Supports different operating systems (Linux, Symbian, Android)
  - Very fast switching between different Compartments and TVDs
- **Contra:**
  - Short development cycles

Towards Mobile TVDs

Trusted Mobile Desktop

Provides secure GUI and isolation of operating systems and stand-alone trusted applications (e.g., SMS application)

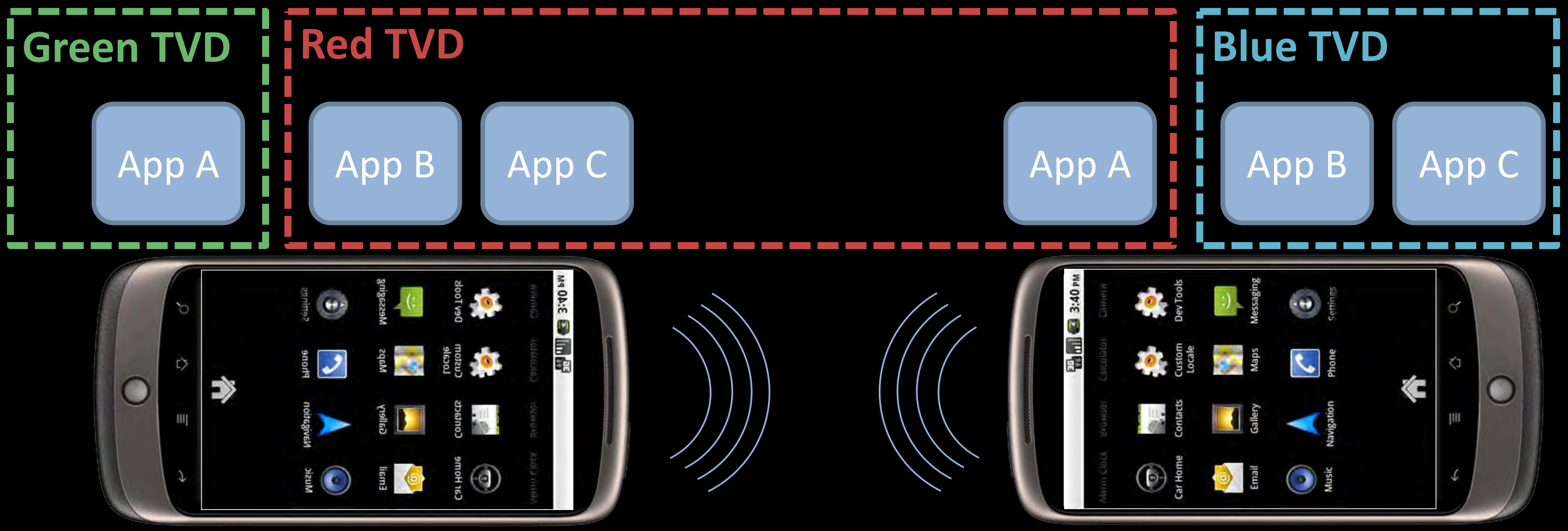


Sirrix Security Technologies

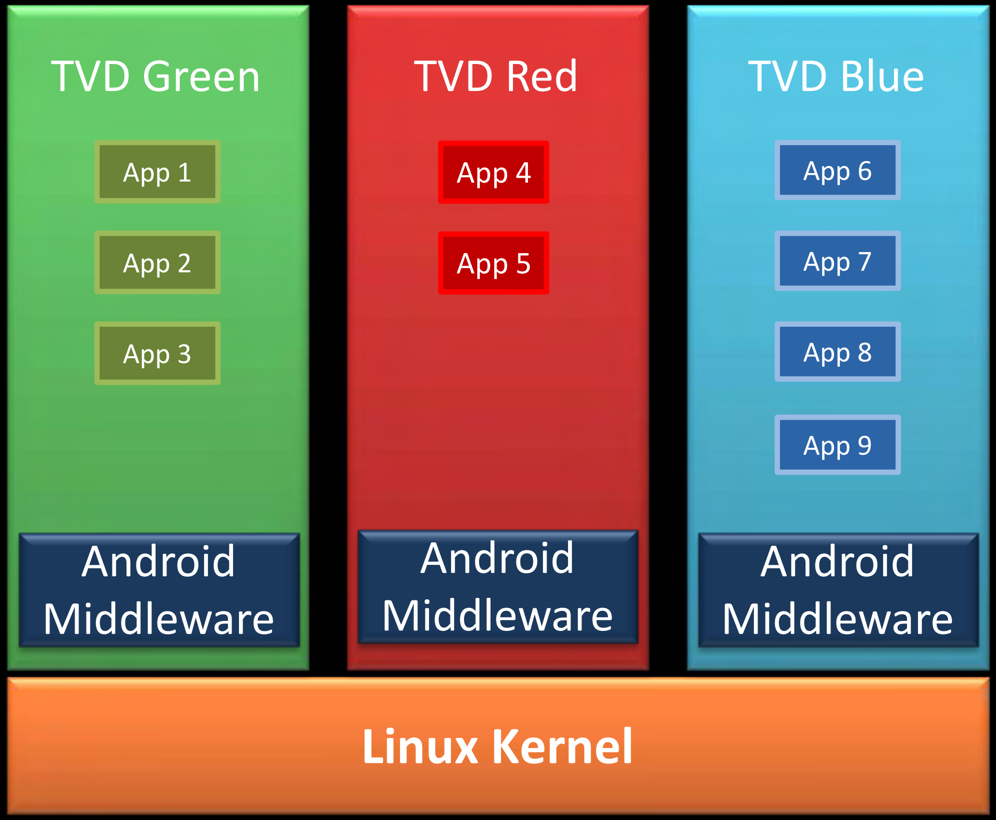
M. Selhorst , C. Stueble, F. Feldmann, U. Gnaida: Towards a Trusted Mobile Desktop. Trust 2010.

System Security Lab Fraunhofer SIT TECHNISCHE UNIVERSITÄT DARMSTADT CASED

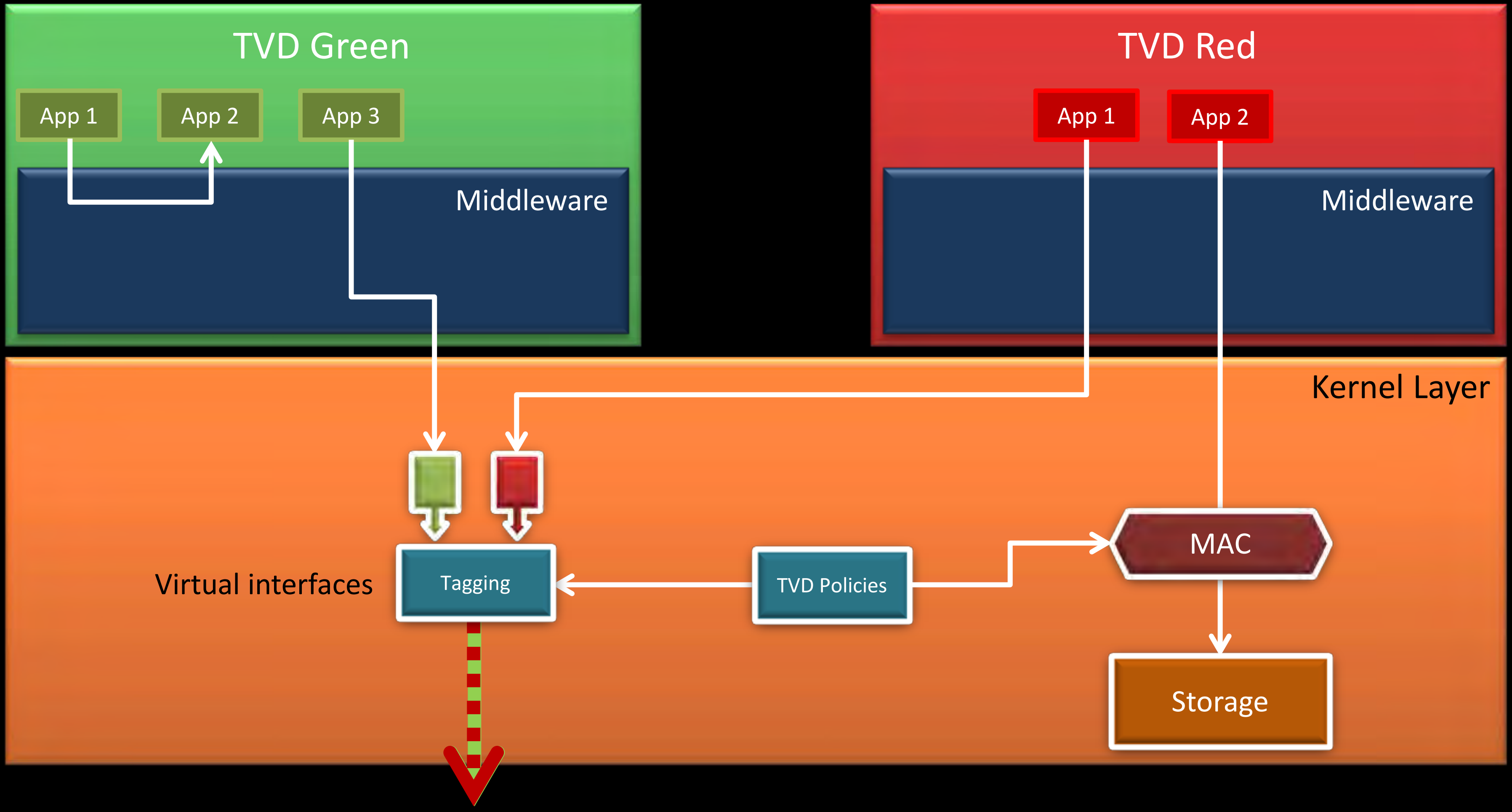
Android TVD: Color your Apps!



Concept: Container Isolation



Isolation with Containers



Medical Data Classification in the Cloud: Is secure computation possible?

www.speedproject.eu

System Security Lab

Fraunhofer SIT

TECHNISCHE UNIVERSITÄT DARMSTADT

CASED

Process Aggregated Medical Data

E-Health Service

Example: Google Health

Patient reveals medical data to e-health provider

Privacy in Google Health

Problem: Googli-Leak
Health learns Patient's Medical Data

WIKILEAKS

➩ **Insider Attacks !!!**

Goal: Reveal no information at all!

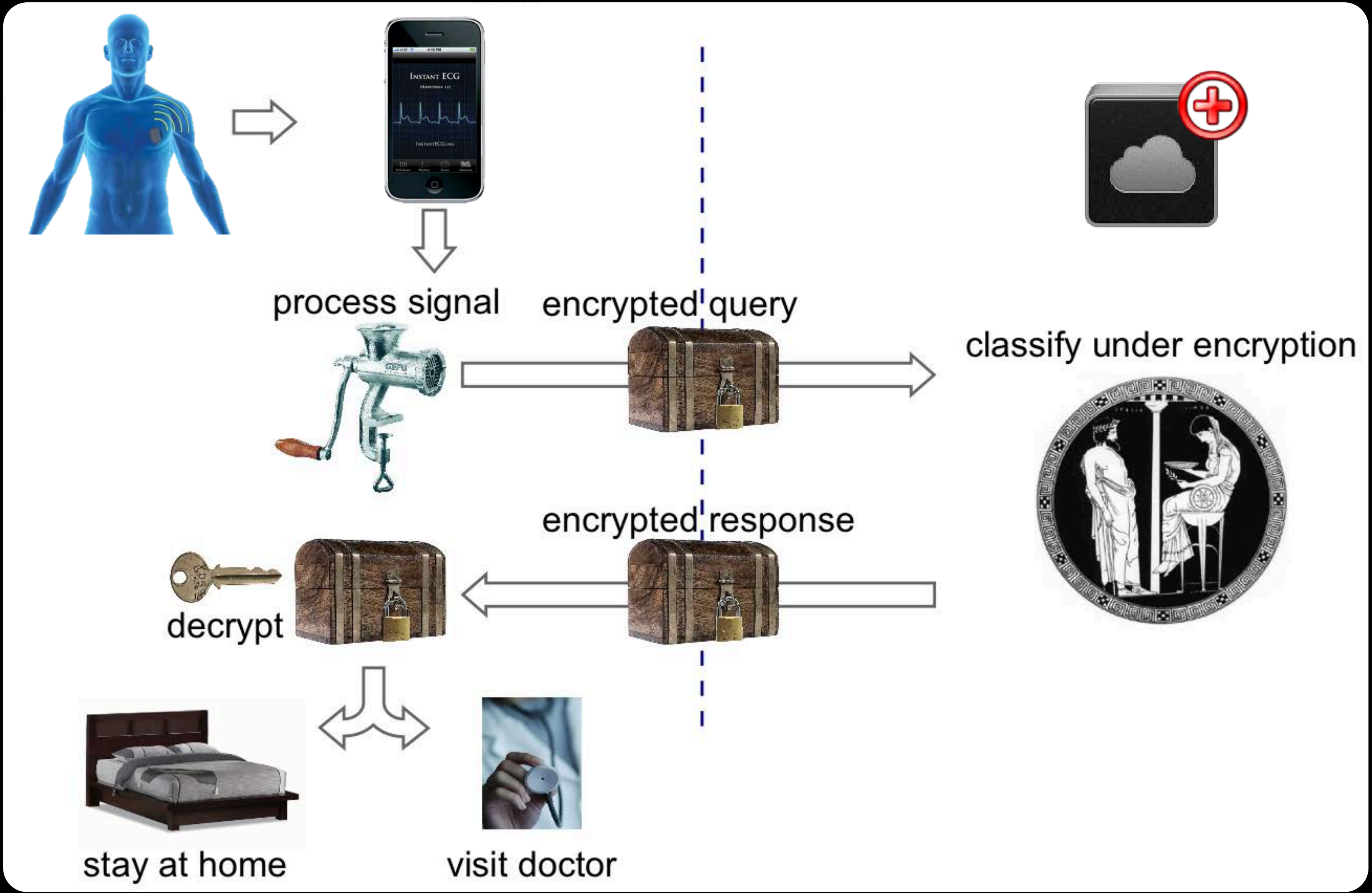
Conflicting Security Objectives

Protect Data

Protect IP

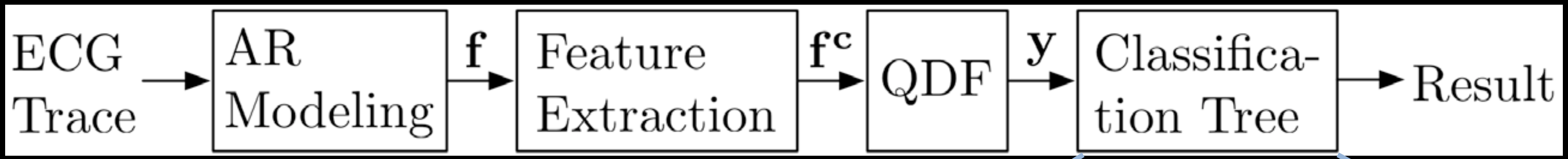
⇨ No trivial solution!

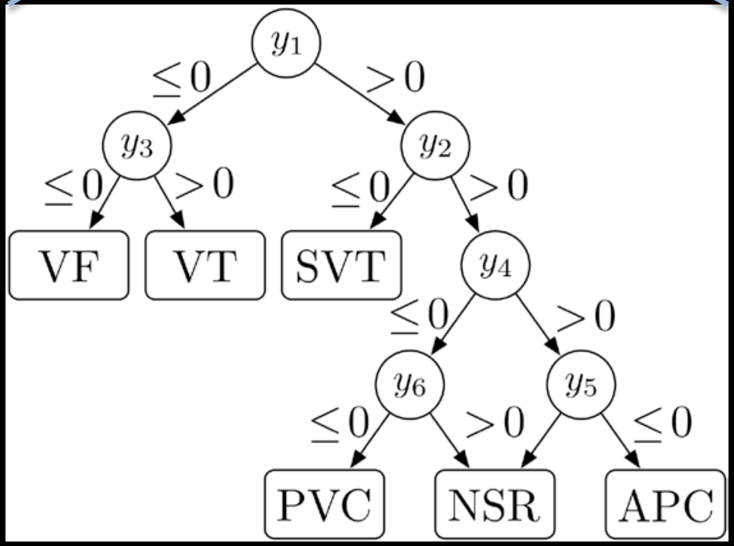
Privacy-Preserving Medical Diagnostics



System Security Lab Fraunhofer SIT TECHNISCHE UNIVERSITÄT DARMSTADT CASED

ECG Classification

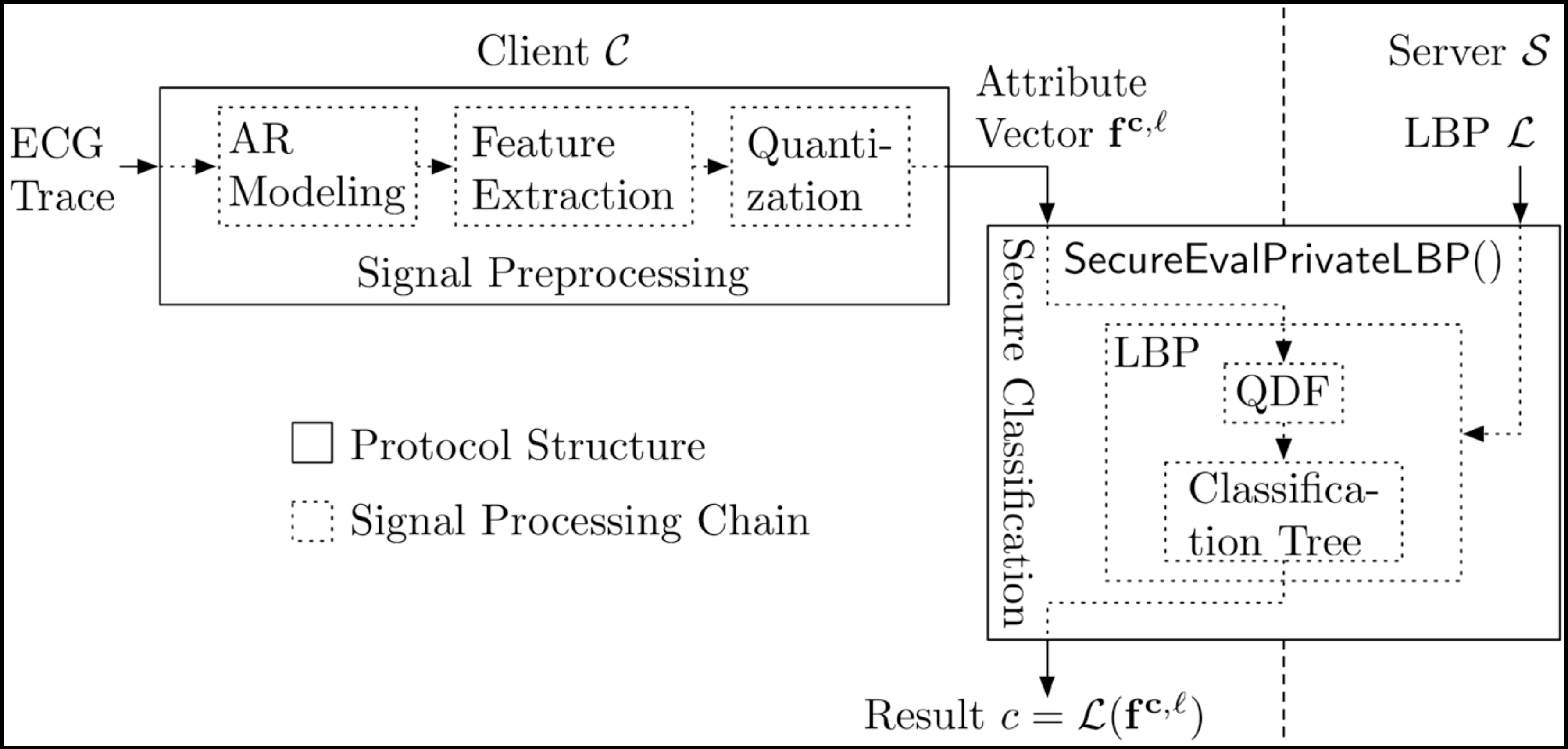




NSR: Normal Sinus Rhythm
APC: Atrial Premature Contraction
PVC: Premature Ventricular Contraction
VF: Ventricular Fibrillation
VT: Ventricular Tachycardia
SVT: Supra Ventricular Tachycardia

U. R. Acharya, J. Suri, A. E. Spaan, S. M. Krishnan. Advances in Cardiac Signal Processing, Springer, 2007

Privacy-Preserving ECG Classification



Privacy-Preserving ECG Classification

- ECG Classification algorithm computed entirely under encryption using combination of efficient techniques for secure computation:
  - Computing with encrypted functions [Yao 1986]
  - Computing on encrypted data [Paillier 1999]

Classification Accuracy	83.3%
Runtime for Secure Classification (excluding signal processing)	18.7s
Communication	64 kByte

On two PCs (3GHz Intel Core Duo, 4GB RAM), Gigabit Ethernet

M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A.-R. Sadeghi, T. Schneider: Secure evaluation of private linear branching programs with medical applications. ESORICS'09.

M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A. Paus, A.-R. Sadeghi, T. Schneider: Efficient privacy-preserving classification of ECG signals. IEEE WIFS'09.

M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, T. Schneider: Privacy-preserving ECG classification with branching programs and neural networks. IEEE TIFS'11 (to appear).

Conclusion and Future Work

- **(I)MDs are becoming reality**
- **Particularly important in aging societies**
- **(I)MDs are subject to counterfeiting**
- **However, (I)MDs are part of the story**
  - Distributed infrastructure
  - Many devices and many parties
  - Cloud availability and secuity
  - Auditing systems
- **Core issues**
  - Privacy by design
  - Legal aspects
  - Emergency regulations
  - Usable security