

From (I)MD to Cloud!



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

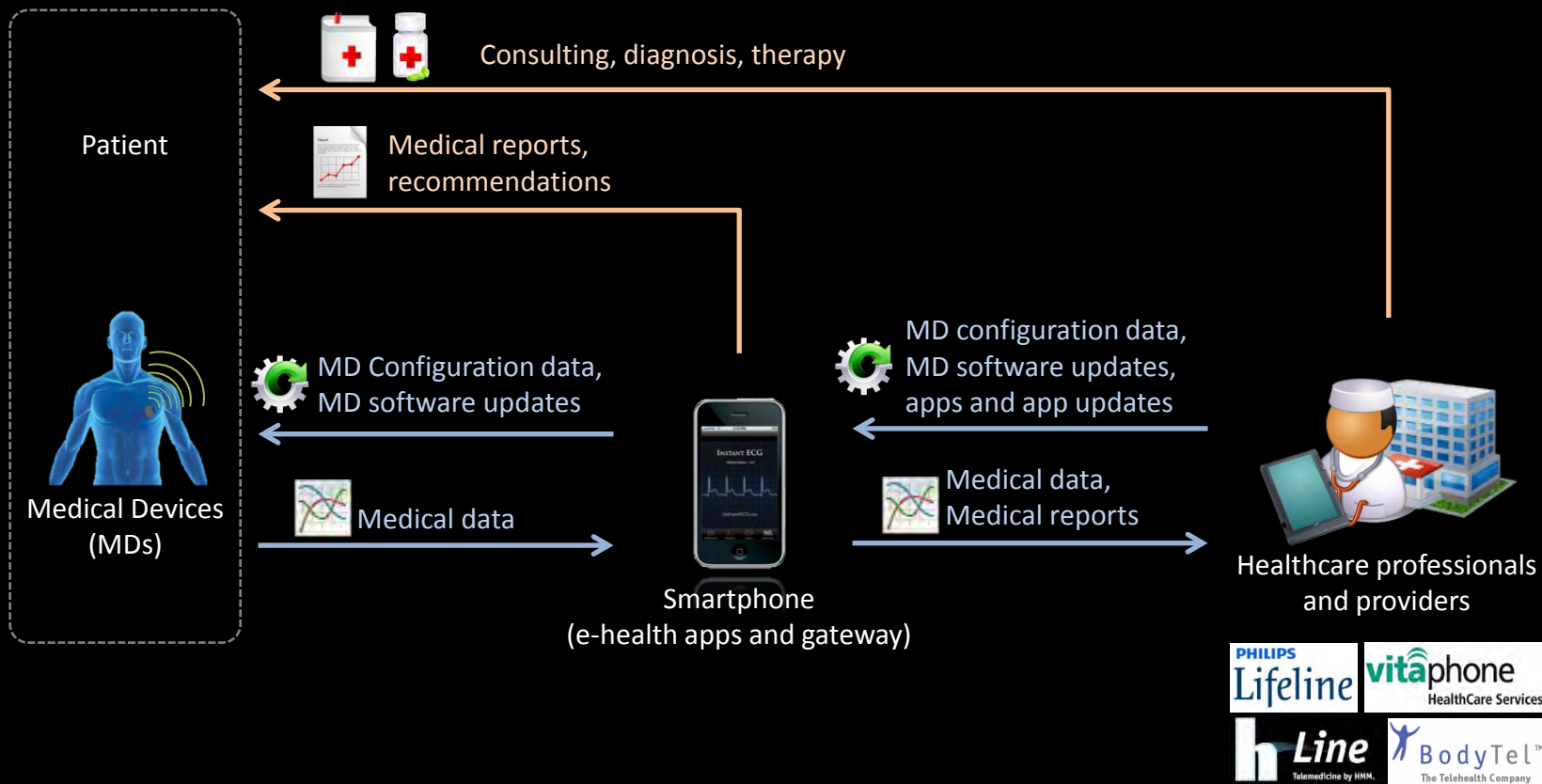
Mina Deng
Philips Research Eindhoven, Netherlands

What is a Cool (I)MD ?



Today: Mobile Health Monitoring

Typically single providers and closed systems

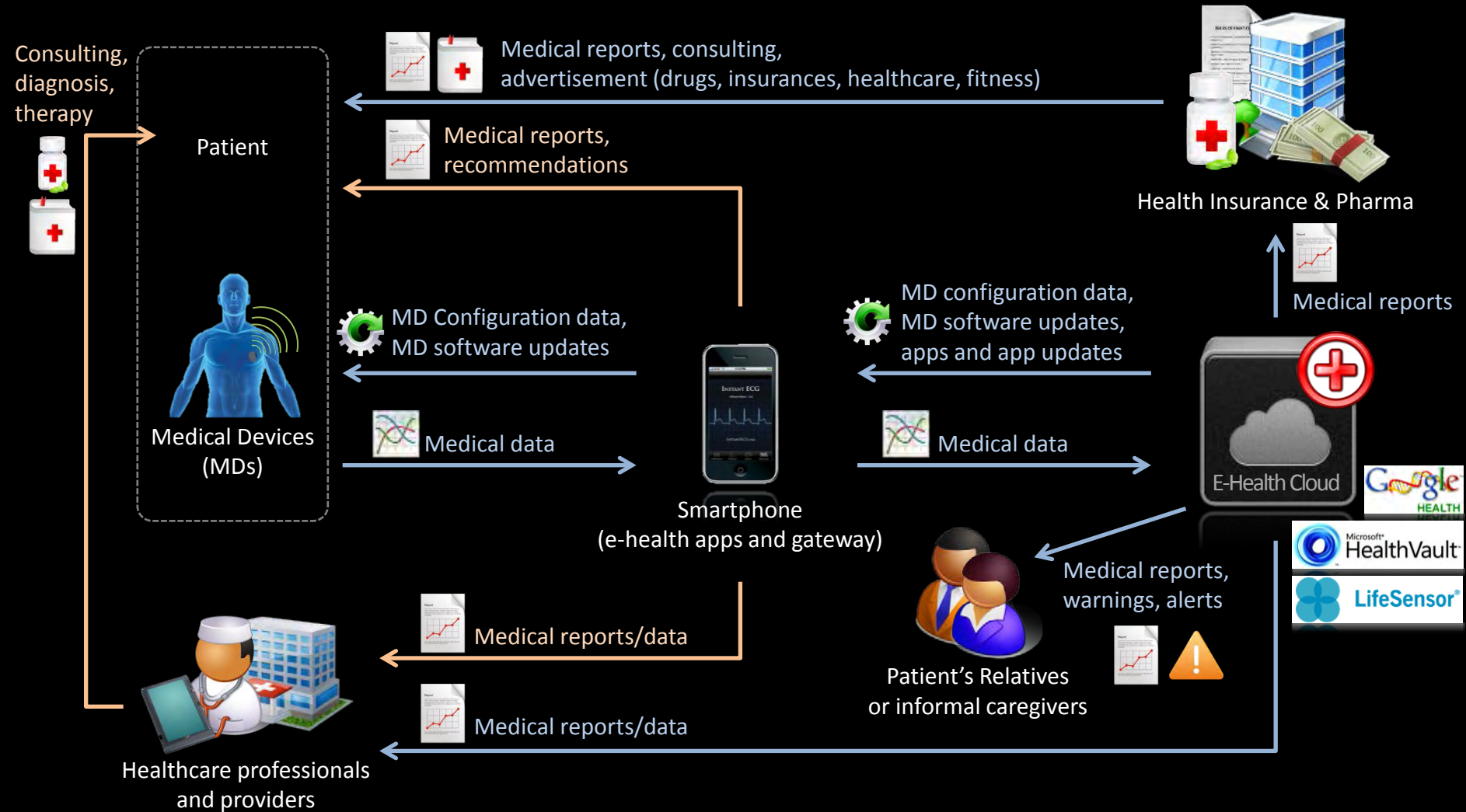


→ Manually initiated by the patient or doctor

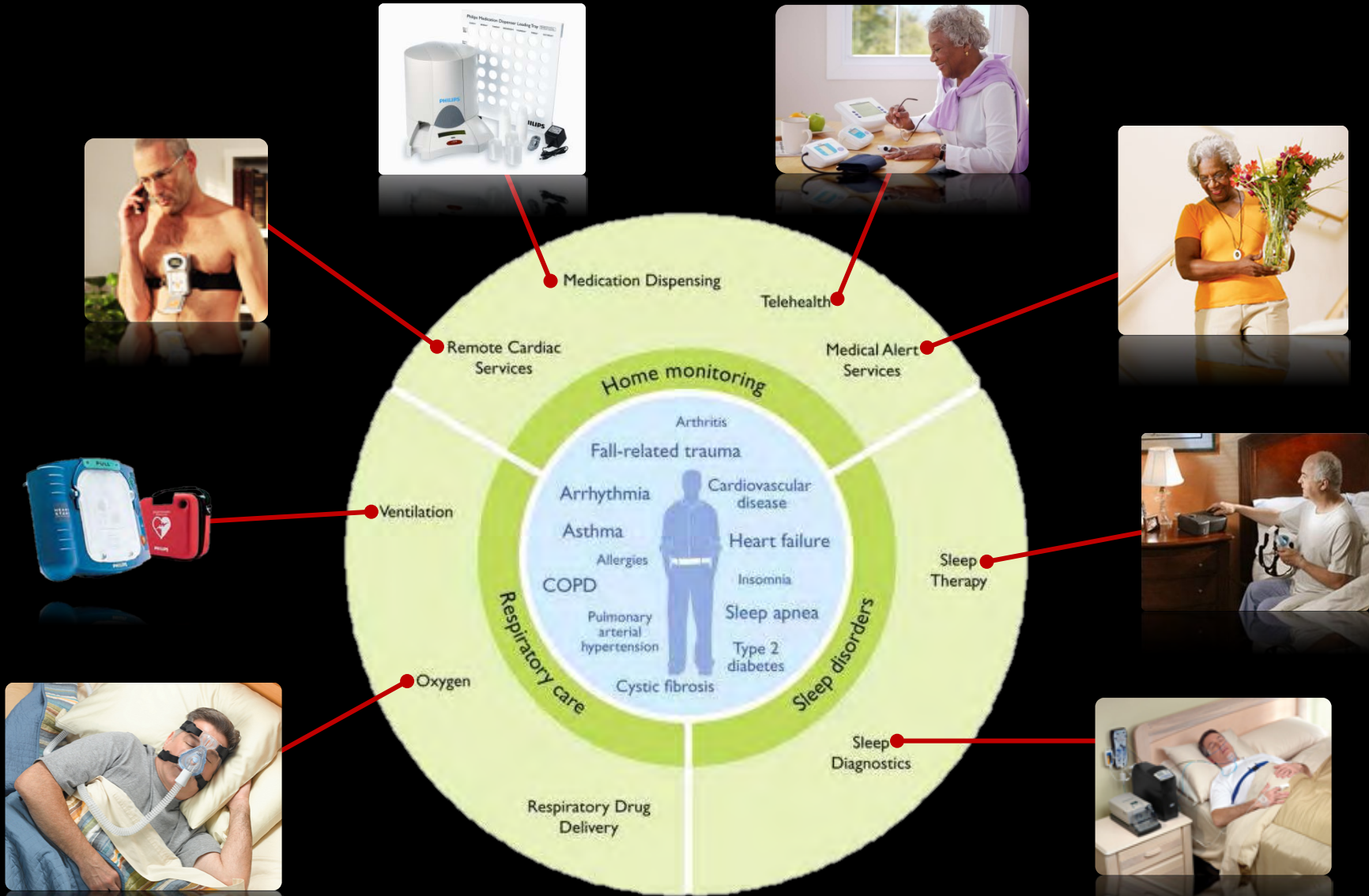
→ No user interaction, fully automatic

Tomorrow: Mobile Healthcare Network

Different providers and distributed systems



Example: Philips Home Healthcare



Objectives and Challenges



Security



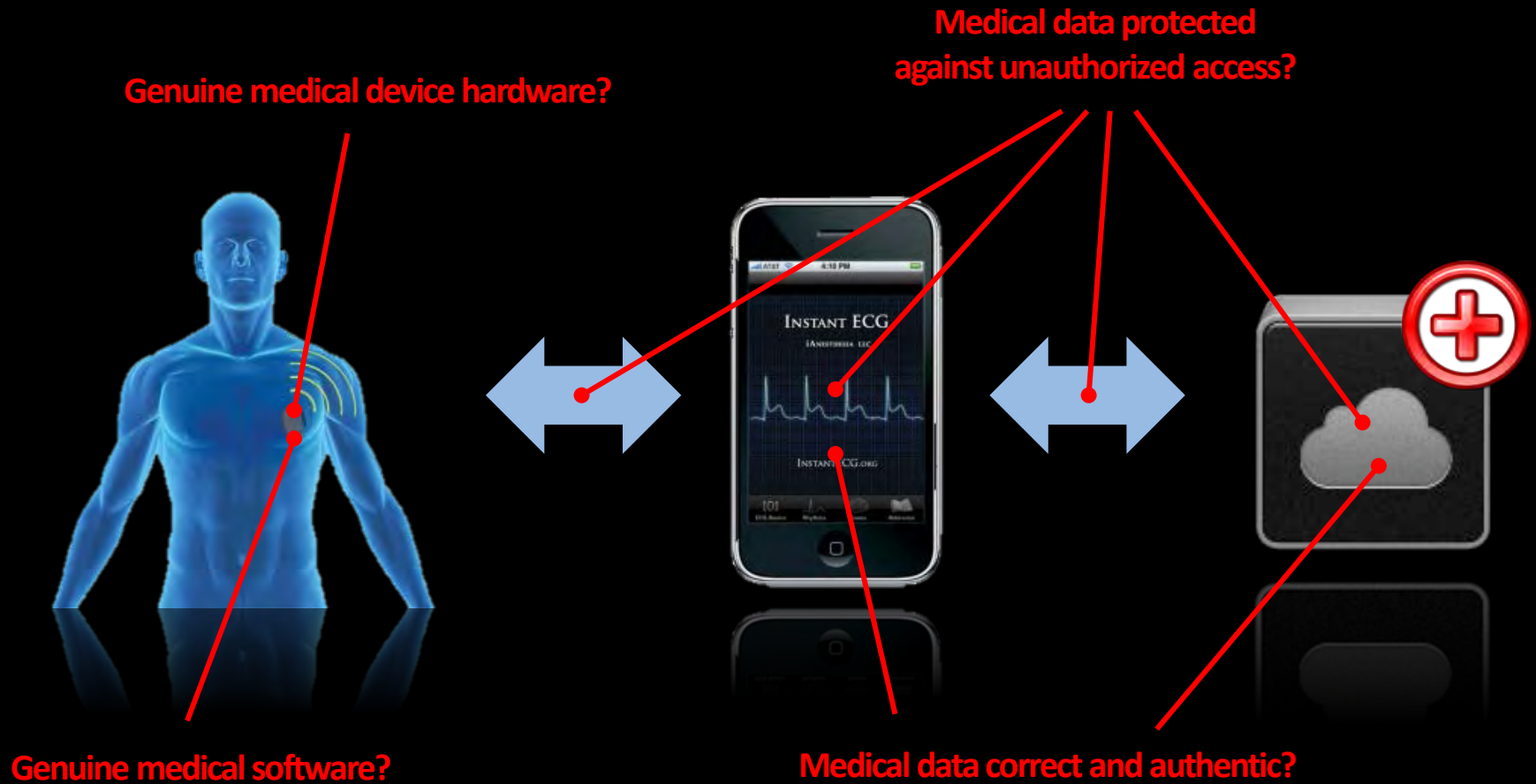
- Data-centric protection
- Semi-trusted cloud service providers (e.g., honest but curious)
- Emergency access and availability
- Reliability, integrity, and confidentiality
- Accountability (incl. integrity of auditing files)
- Efficiency
- Self-management (resilience, availability, adaptability, scalability)

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?



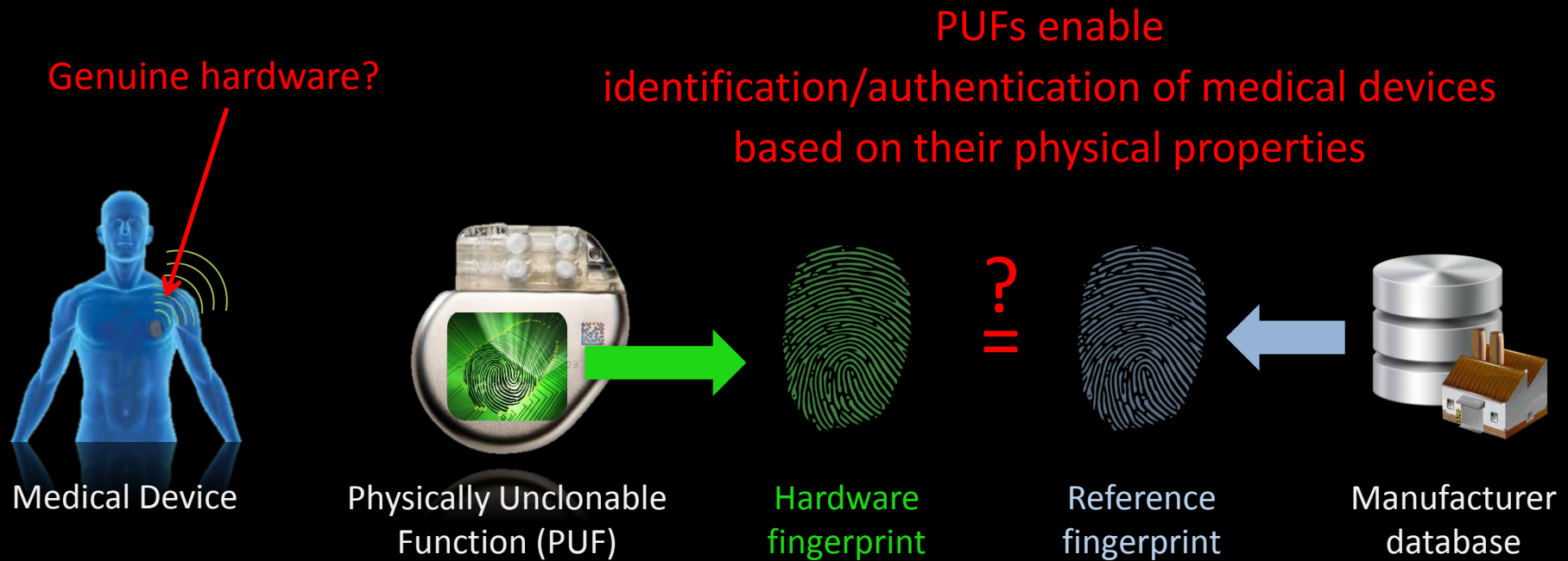
As per an estimate of the OECD and WHO, around 6-8% of the total medical devices market comprises of counterfeit goods.

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.

The screenshot shows the homepage of medicaldevice-network.com. The header includes the site logo, a navigation menu with 'Home', 'Special Features', and 'Phase out the Fakes', and a search bar. The main content area features an article titled 'Phase out the Fakes' with a sub-headline 'Medical counterfeiting globally is rife, with only a fifth of countries having strict regulations to prevent forgery. Jayant Singh of Frost & Sullivan examines the reasons why such a practice must be stopped.' The article date is '04 Apr 2008'. Below the text are icons for 'Email Article', 'Print', and 'Link To Us'. A sidebar on the left lists 'New On This Site', 'Products & Services', 'Company A-Z', 'Case Studies', 'Special Features' (highlighted), and 'White Papers'. A sidebar on the right promotes 'MyTrainingExpert' as 'The UK's Largest Buyer of Training Courses'.

Physical Device Identification



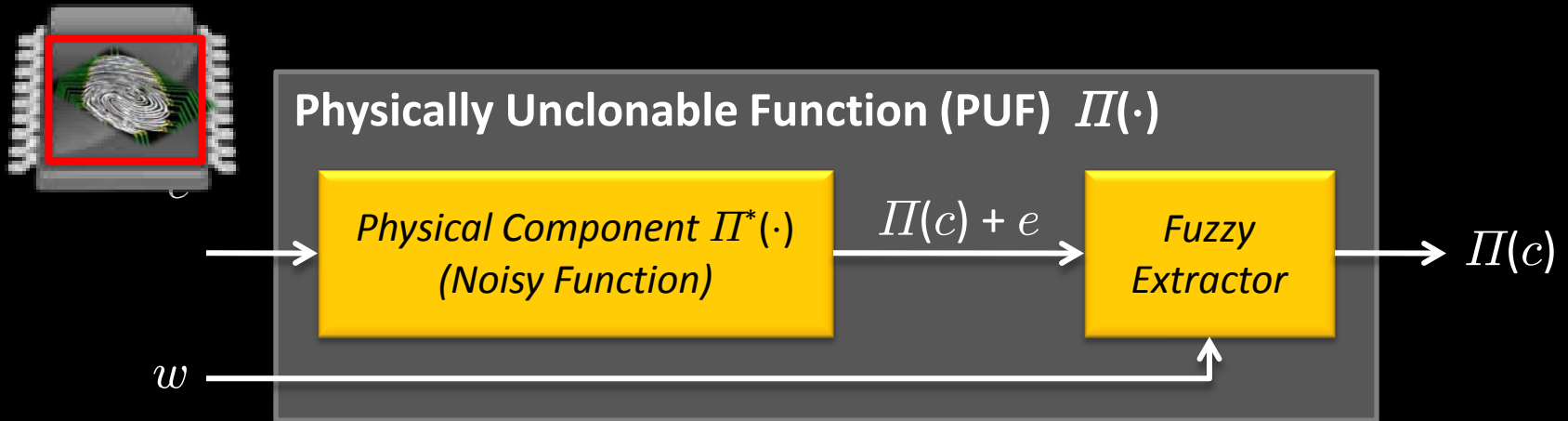
Assumptions

- 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

Physically Unclonable Functions



c Challenge

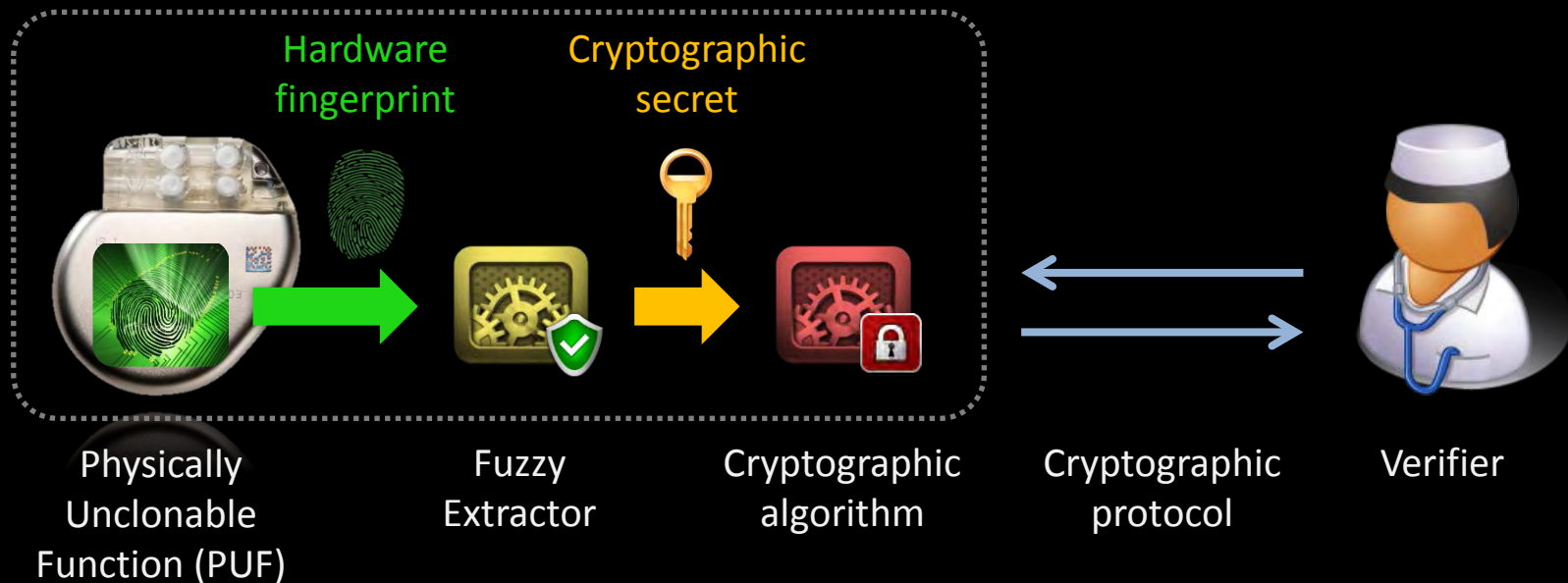
e Error (noise) of Π^*

w Helper data

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

PUF-based Key Storage

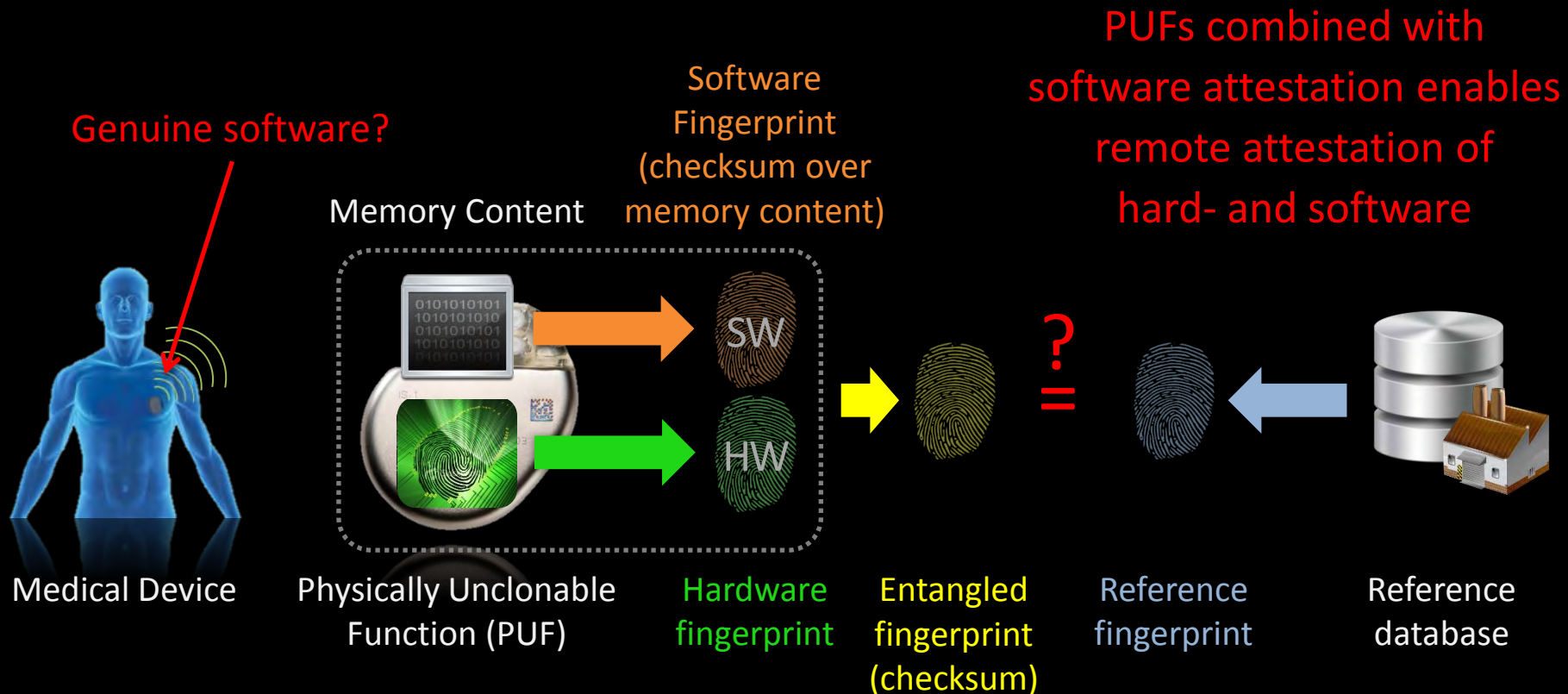
[Šcoric et al. 05, Lim et al. 05]



Assumptions

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

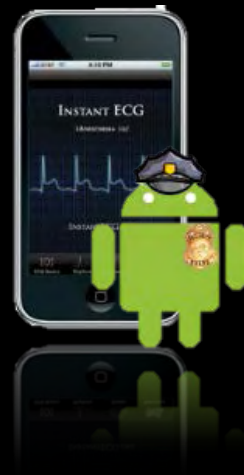
Software Integrity Verification



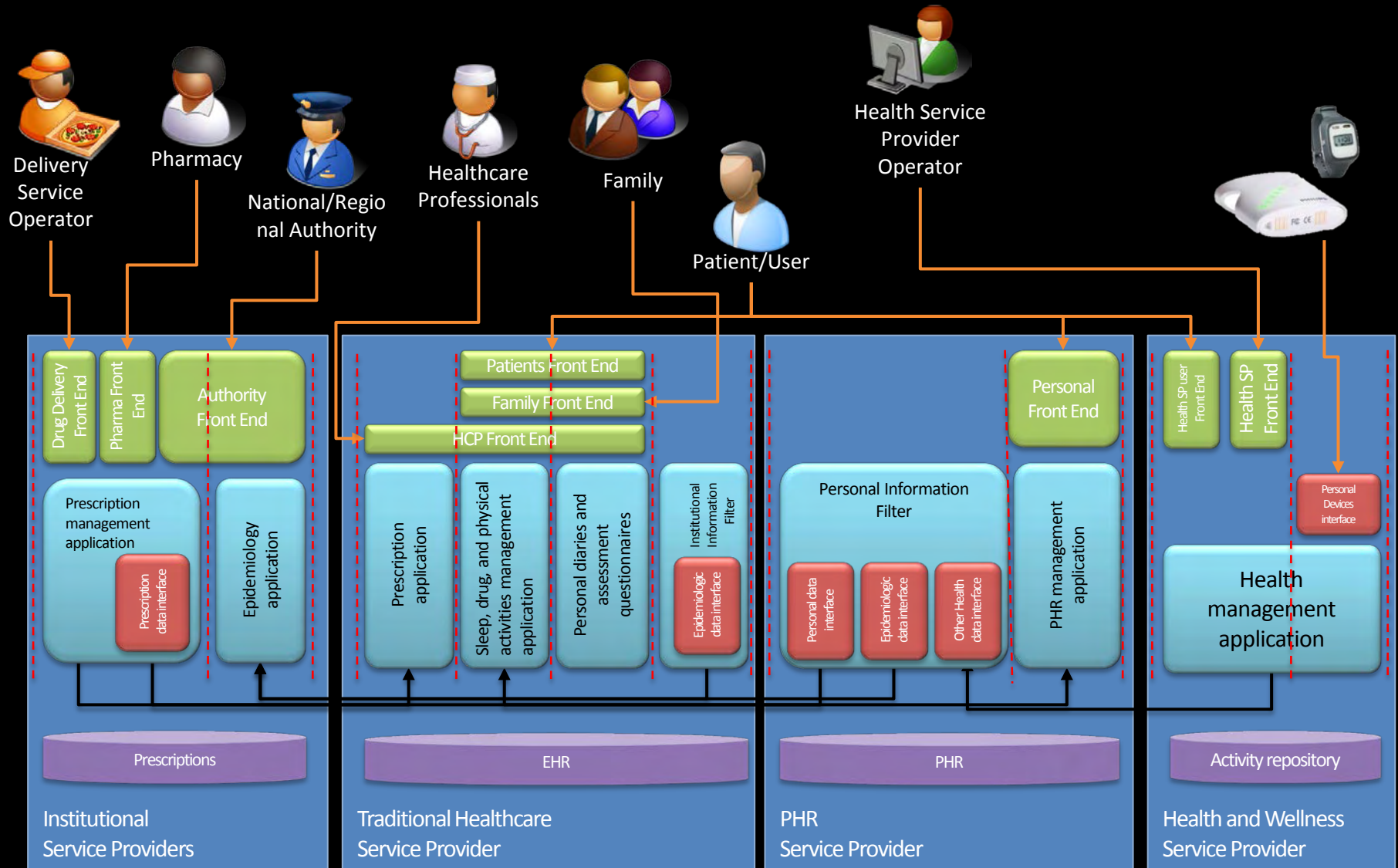
Assumptions

- 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)

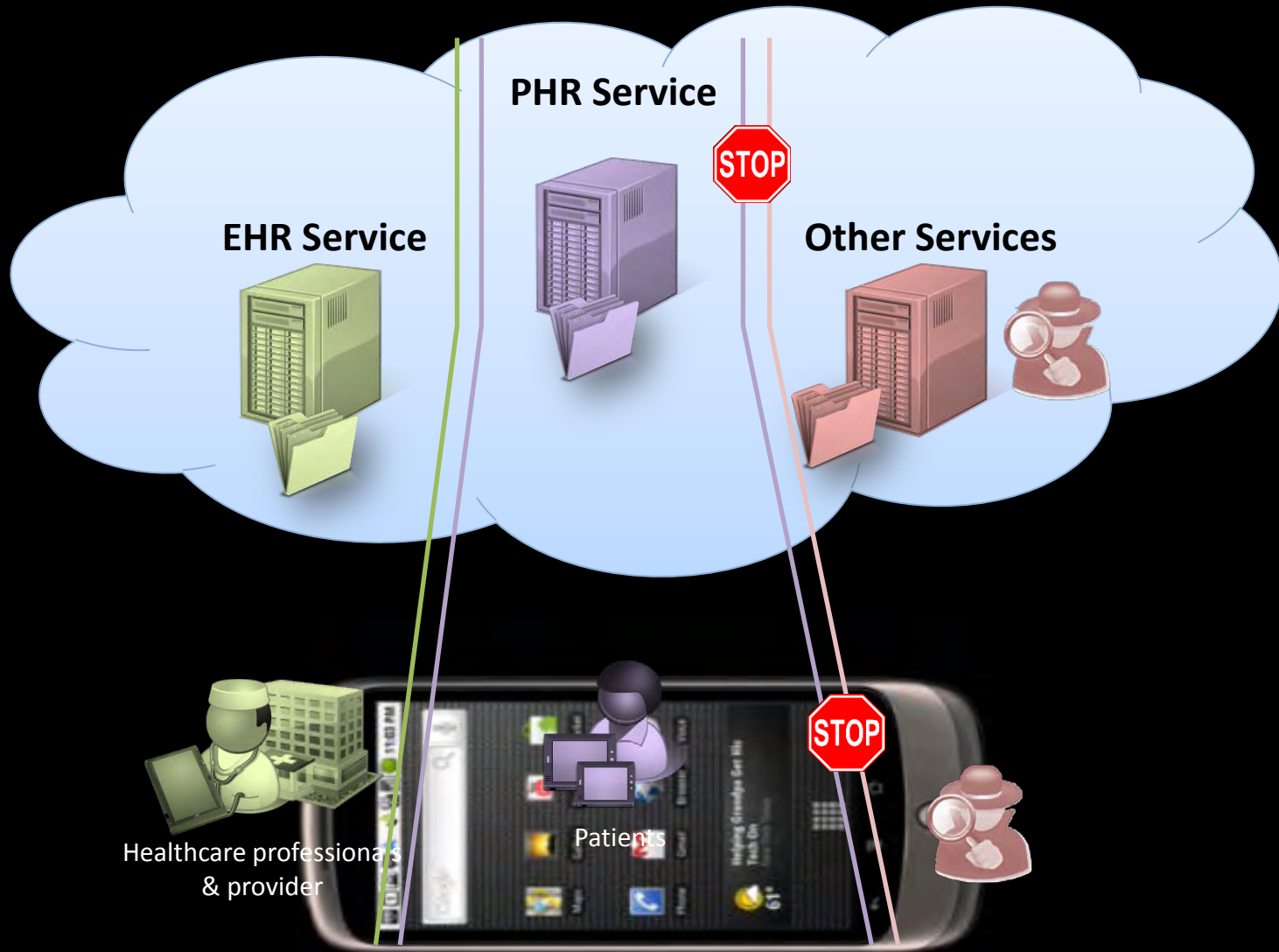
Medical Infrastructure Security: Who, when, where access data?



Conceptual Architecture: Global View



Privacy Domains

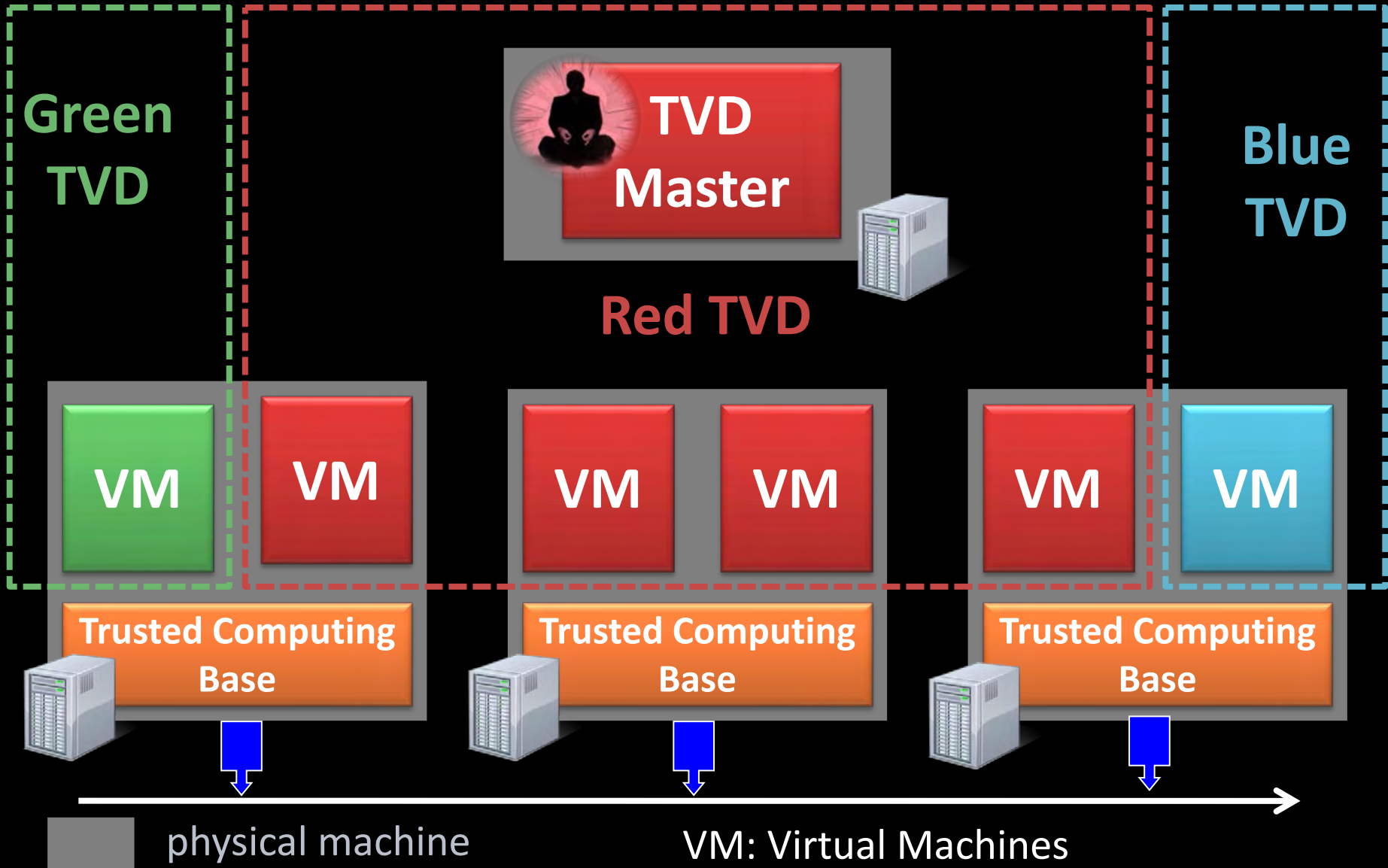


Technology: Trusted Virtual Domains (TVDs)

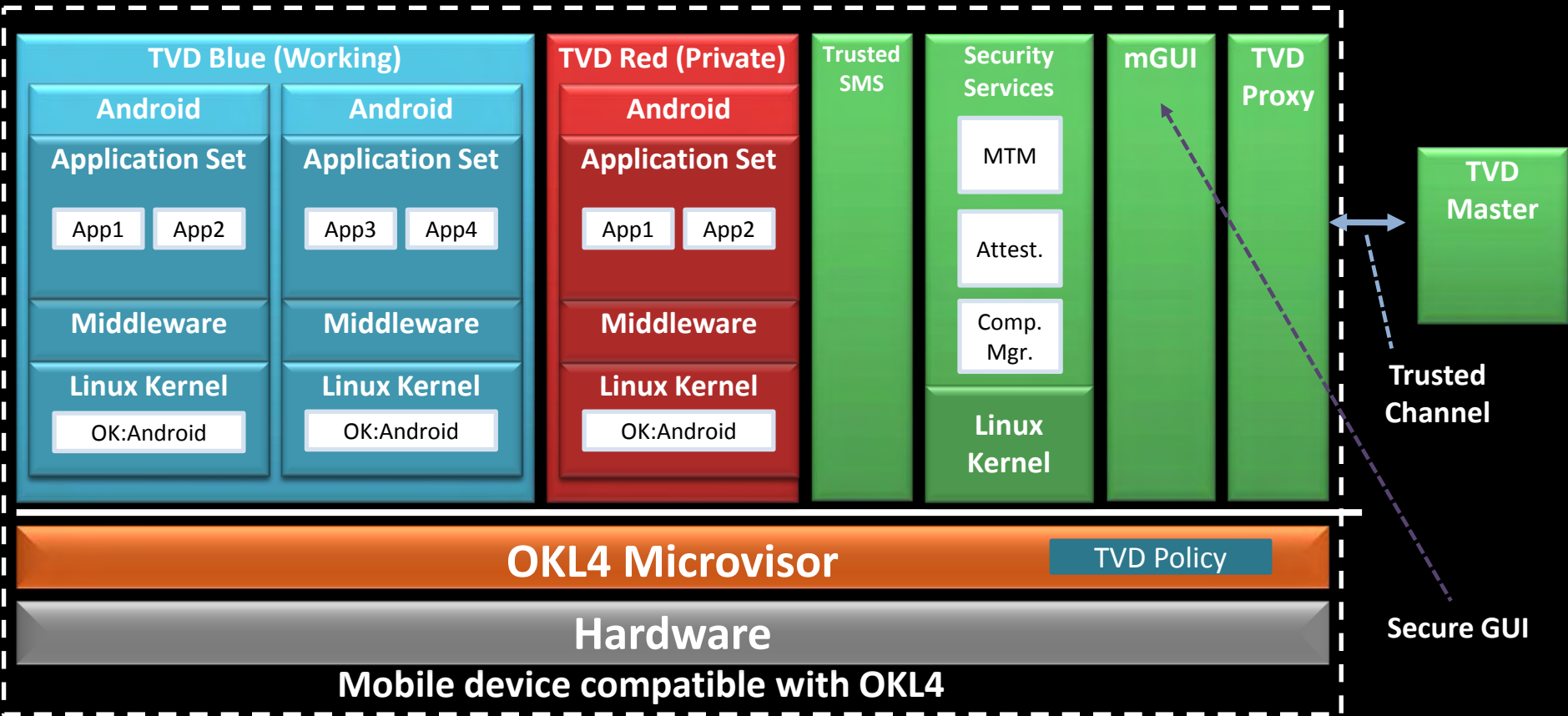


- **TVD = Coalition of virtual machines**
- **Properties**
 - Isolated execution environments (compartments)
 - Trust relationships
 - Transparent policy enforcement
 - Secure communication
 - Client platform security (based on modern hardware security functionality)

Logical TVD Architecture



Integration of TVD Main Components



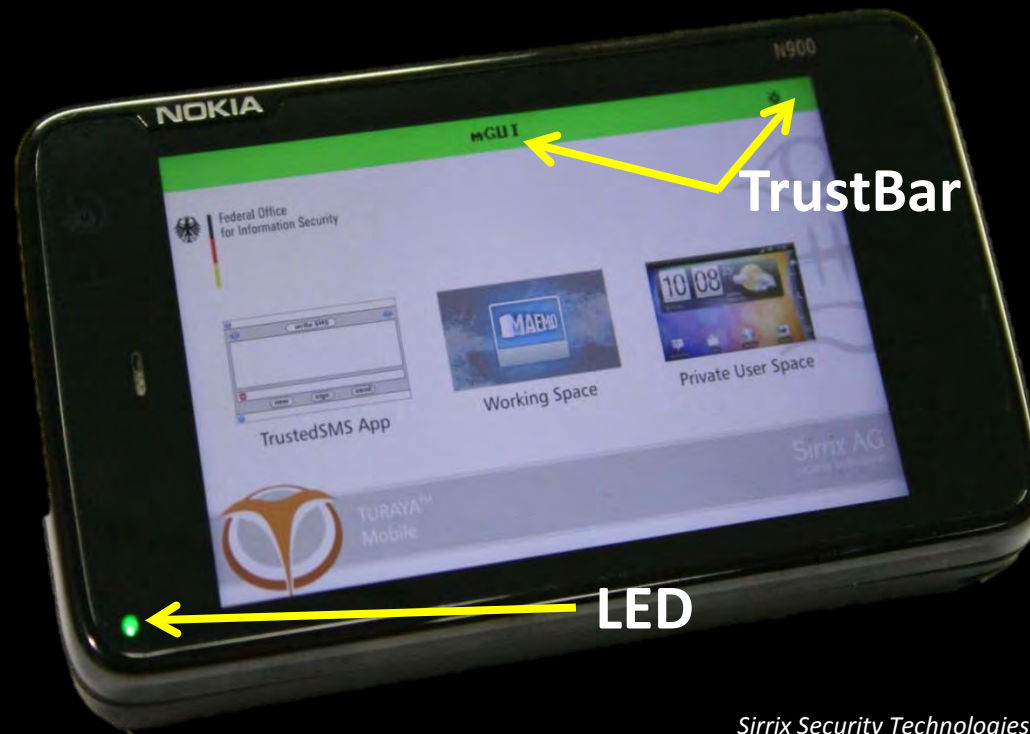
Pro and Contra

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

Towards Mobile TVDs

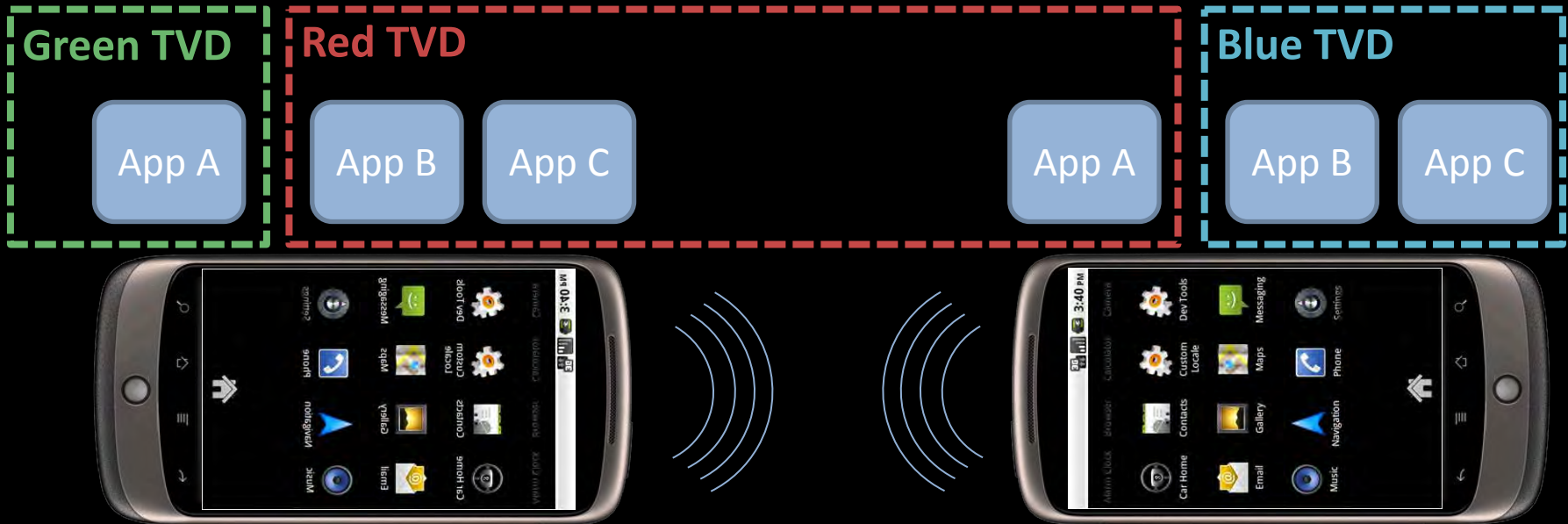
Trusted Mobile Desktop

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

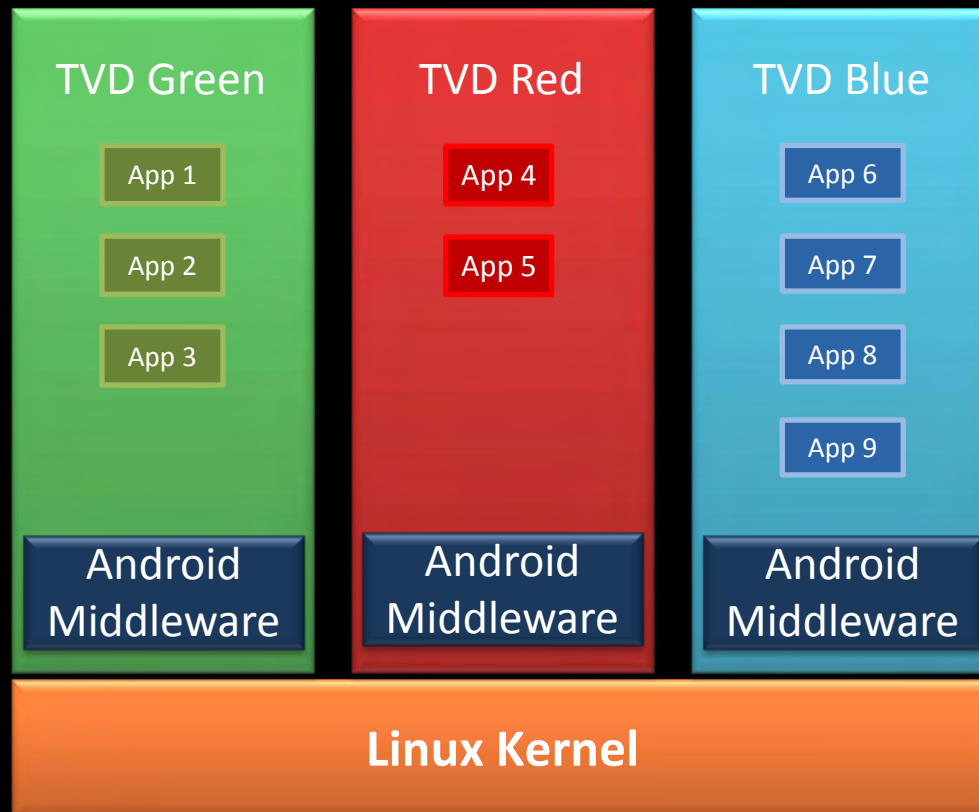


Sirrix Security Technologies

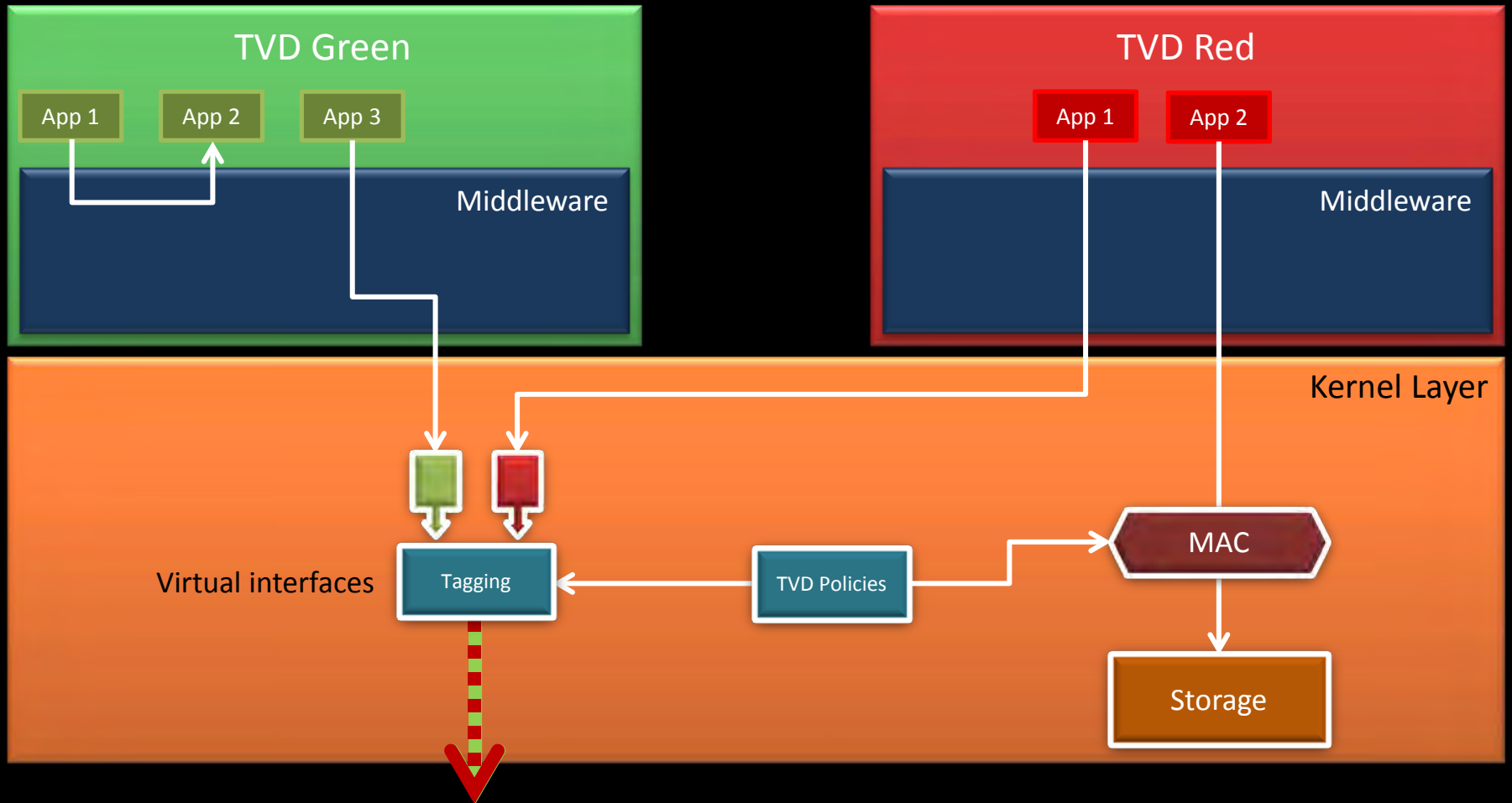
Android TVD: Color your Apps!



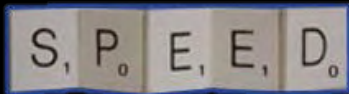
Concept: Container Isolation



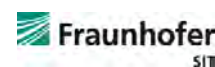
Isolation with Containers



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



www.speedproject.eu



Process Aggregated Medical Data



Example: Google Health

Google health Search the Web [Browse all health topics](#) [Take our survey!](#)

Profiles: **Unnamed profile** [Options](#) [Print](#) [Download](#) [Share](#) [Private](#)

Unnamed profile [Edit](#)
Age: unknown | Sex: unknown | Race / Ethnicity: unknown | Blood type: unknown

Summary [All records](#)

Wellness [Hide wellness](#)

- Blood pressure (0)
- Hours slept (0)
- Steps taken (0)
- Weight (with BMI) (0)

[Remove from summary](#) [Data reviewer](#)

Problems [Add](#)
Keep a history of ailments, conditions, or symptoms you've experienced (past and present).

Medications [Add](#)
List all your prescriptions, supplements, vitamins, and over-the-counter drugs.

Allergies [Add](#)
Report the medications, foods, and environmental triggers that cause your allergies.

Test results [Add](#)
Track any test results, diagnostics, screenings, or evaluations from your medical providers.

Procedures [Add](#)
Keep a history of any inpatient or outpatient procedures and surgeries.

Immunizations [Add](#)
Record any vaccinations you've received.

Insurance [Add](#)
Keep a handy list of your medical, dental, and vision insurance.

Files [Choose File](#) no file selected
Maximum file size: 4 MB
Add any documents or images with health information.

Personalize this profile
We created this profile to help you get started. Customize it to manage health information for yourself or someone you care for. Add details, import records, or explore tools to get the most from your health information.
[Dismiss this tip](#) | [Learn more](#)

Updates [Check now](#)
[Notices \(0\)](#) - [Activity report](#)

Import medical records [?](#)
Plus get automatic updates when something changes.
[Browse all 25 import sources](#)

Put your information to work [?](#)
Sign up for personalized news, advice, and other tools. Most are free.
[Browse all 38 services](#)

Medical contacts

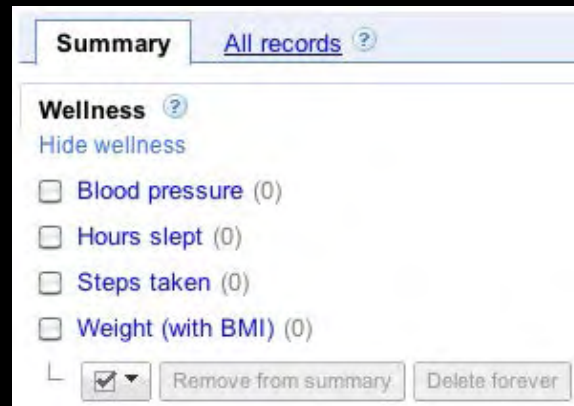
How should Google send alerts and important security notifications?
[Email only](#) [US Mail](#)

Patient reveals medical data to e-health provider

Privacy in Google Health

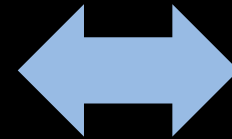
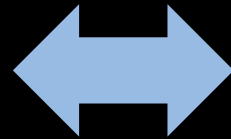
Problem: Googli-Leak
Health learns Patient's Medical Data

⇒ Insider Attacks !!!



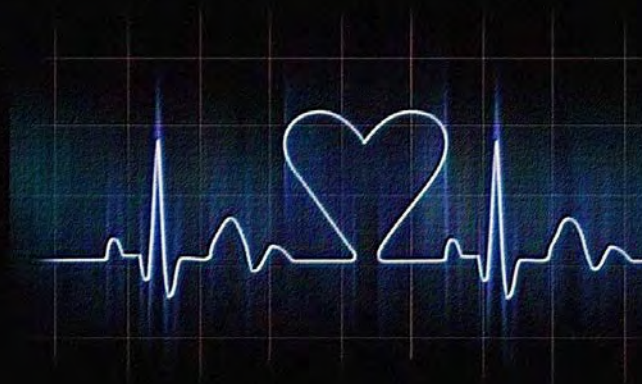
Goal: Reveal no information at all!

Conflicting Security Objectives



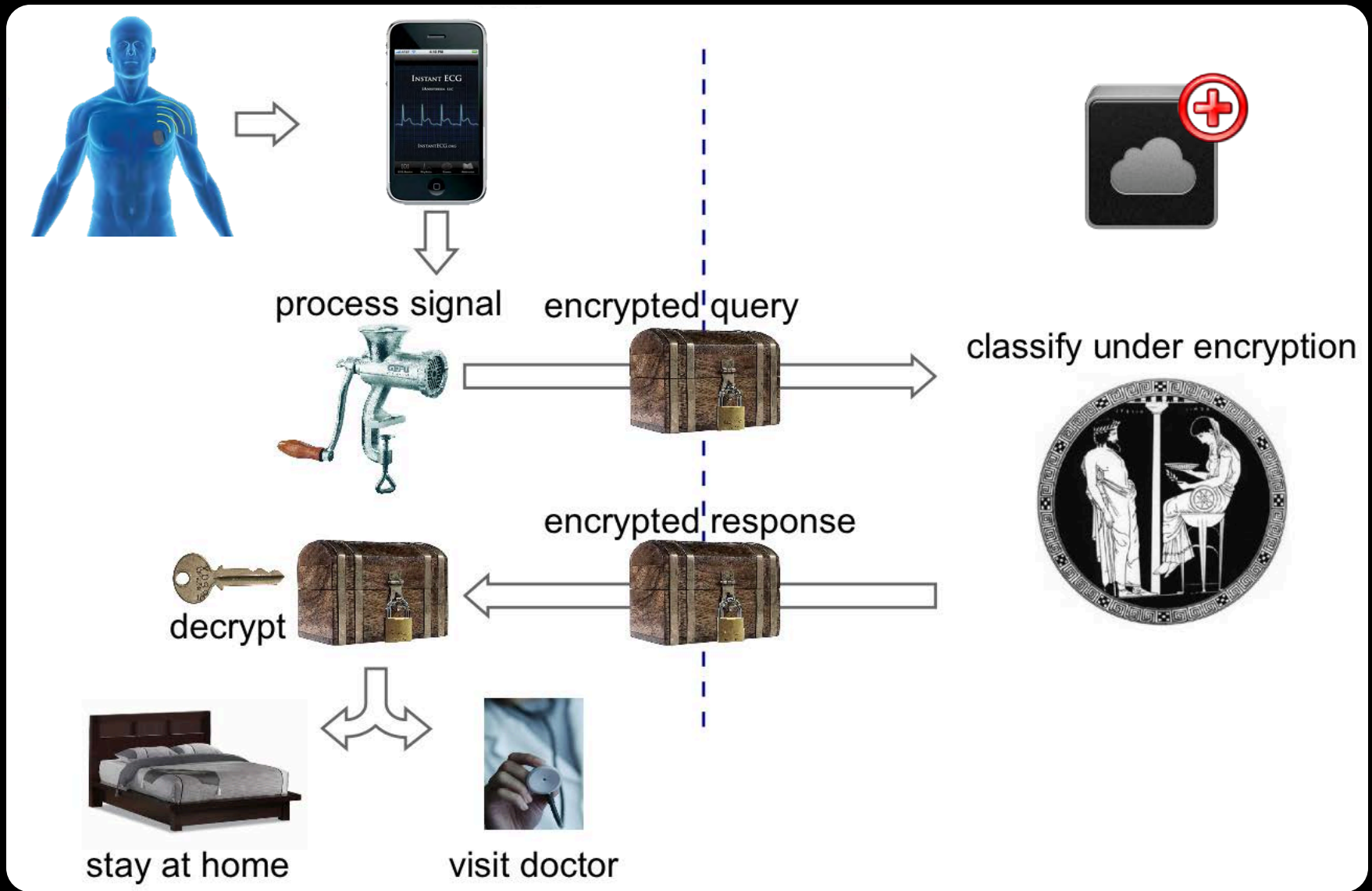
Protect Data

Protect IP

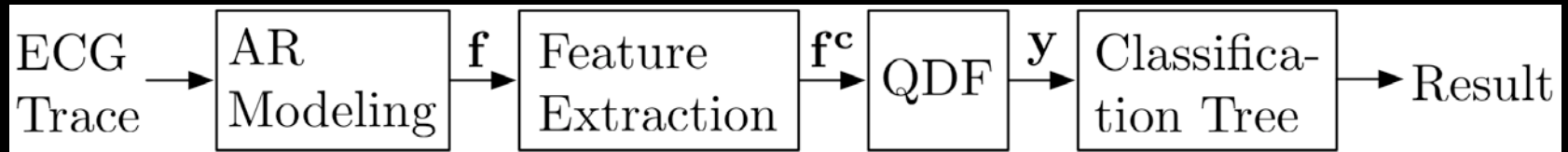


⇒ No trivial solution!

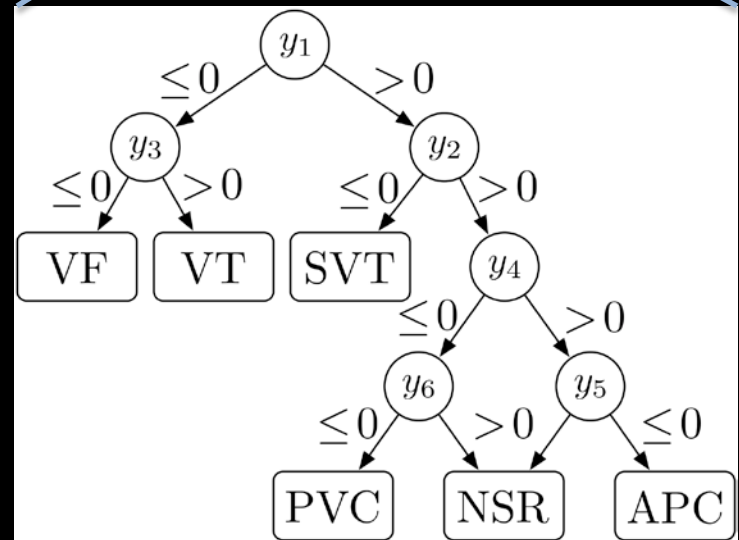
Privacy-Preserving Medical Diagnostics



ECG Classification

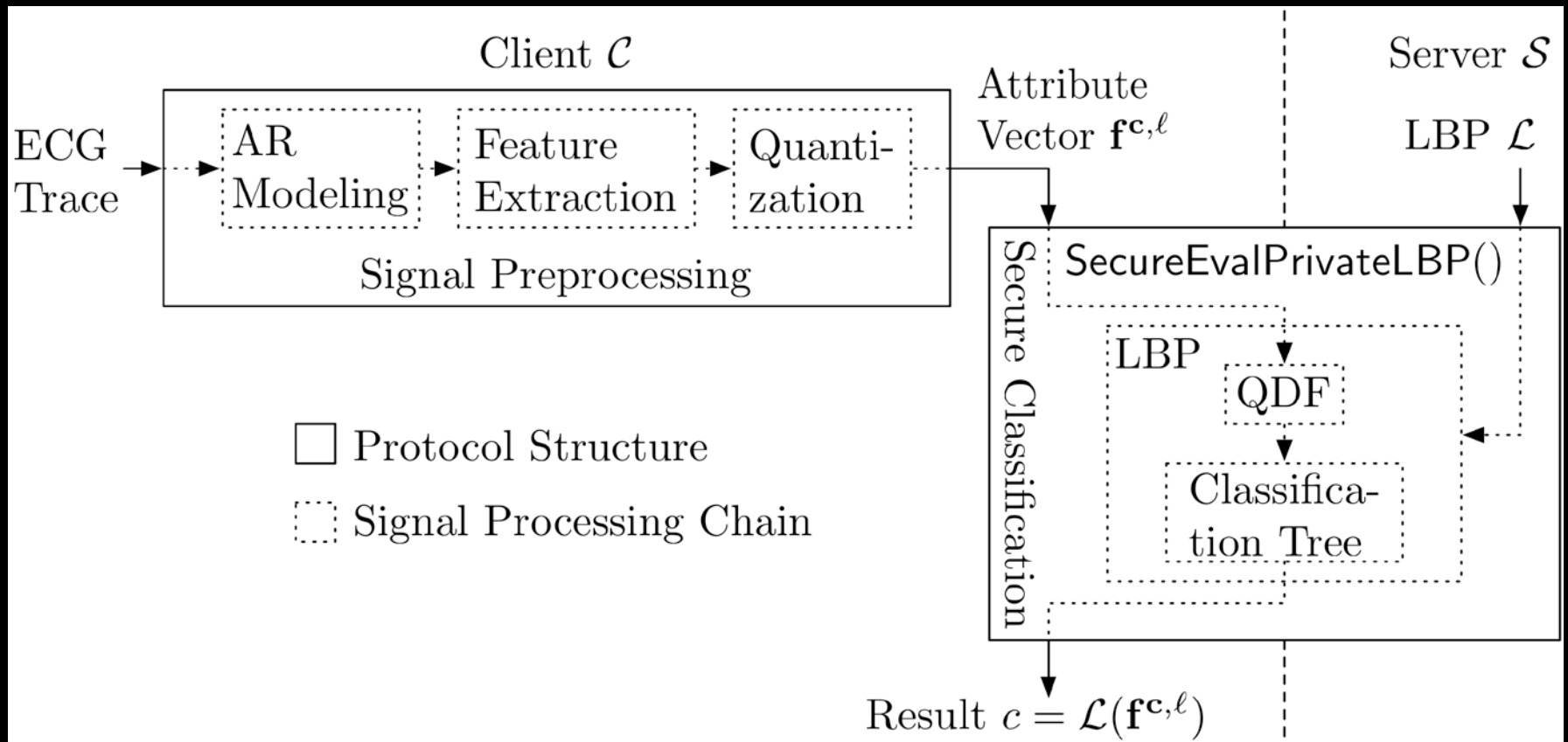


NSR: Normal Sinus Rhythm
APC: Atrial Premature Contraction
PVC: Premature Ventricular Contraction
VF: Ventricular Fibrillation
VT: Ventricular Tachycardia
SVT: Supra Ventricular Tachycardia



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 security
 - Auditing systems
- **Core issues**
 - Privacy by design
 - Legal aspects
 - Emergency regulations
 - Usable security