PHILIPS

sense and simplicity

Security in Consumer Electronics

Paul Thijssen
Philips Applied Technologies

SASG Meeting of February 3, 2009

An introduction to Philips Applied Technologies

Contract R&D services

Innovation through turnkey solutions and specialist support

Healthcare

- Medical devices & implants
- Patient monitoring & connected care
- Medical imaging & therapy systems
- Molecular healthcare devices

Lifestyle

- Multimedia Experience
- Personal Care, Wellness & Beauty
- Robotics
- Information, Storage & Streaming & Retrieval

Technology

- Home and Building Automation & Security
- Instrumentation & Stages
- Opto-electronic modules
- RFID
- Energy

Customers

PHILIPS

Philips Consumer Lifestyle
Philips Lighting
Philips Healthcare
Philips Research
Philips Incubators
Philips IP&S

SONION

JABIL

VISTAKON®
Division of Johnson & Johnson Vision Care, Inc.

NASA

Cochlear™

TRIXELL

Varibel

BOSCH

STORK®

BANG & OLUFSEN

THALES

YAMAHA

Assembléon
Integrated electronics manufacturing solutions

ASML

hp®
invent

Solland

AKZO NOBEL

SKF

océ

NXP
founded by Philips

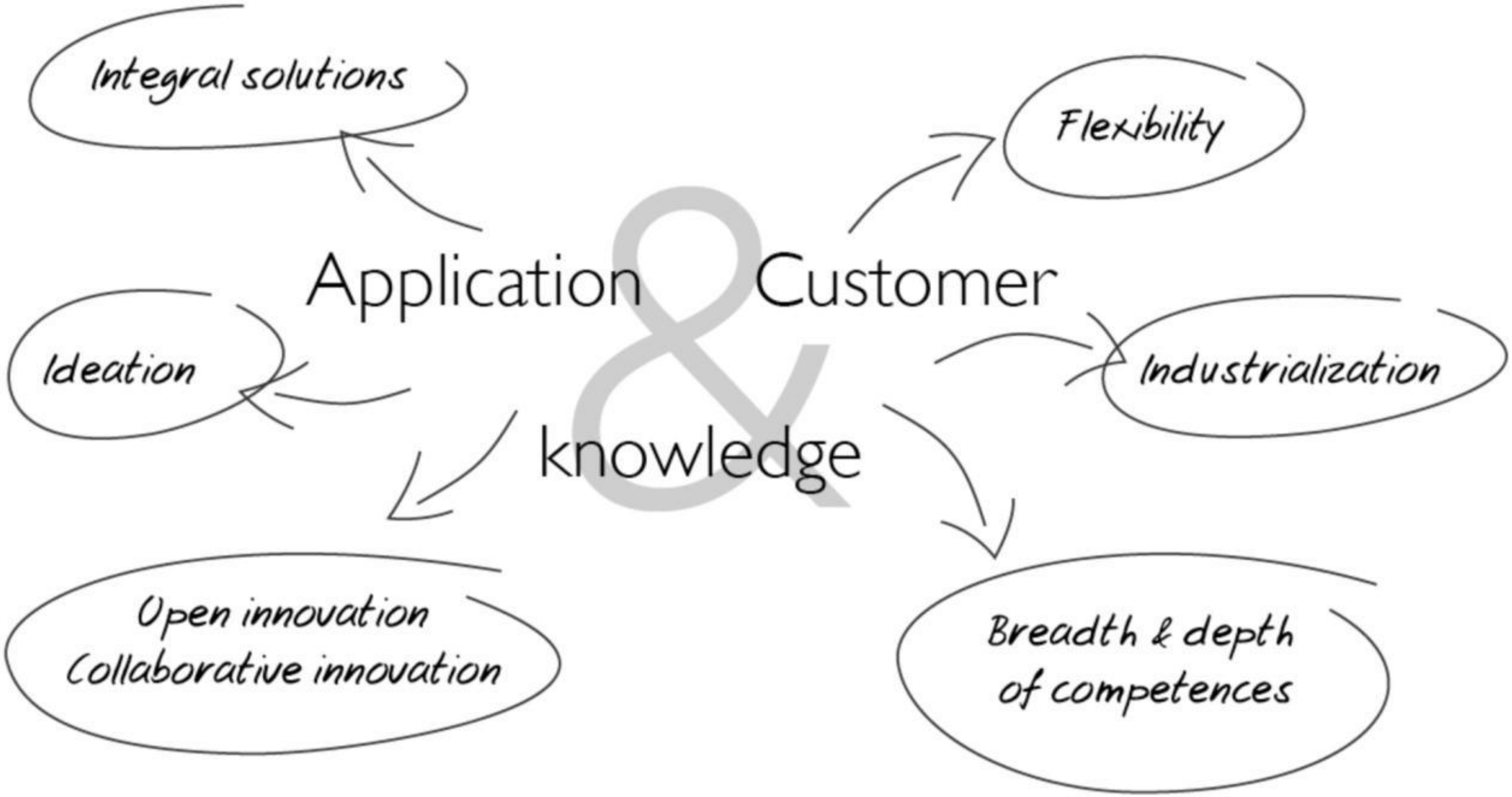
PPG
PPG Industries

Schneider
Electric

KLA Tencor

Tyco Electronics

What we bring to our customers



PHILIPS

At the heart of leading innovations

PHILIPS

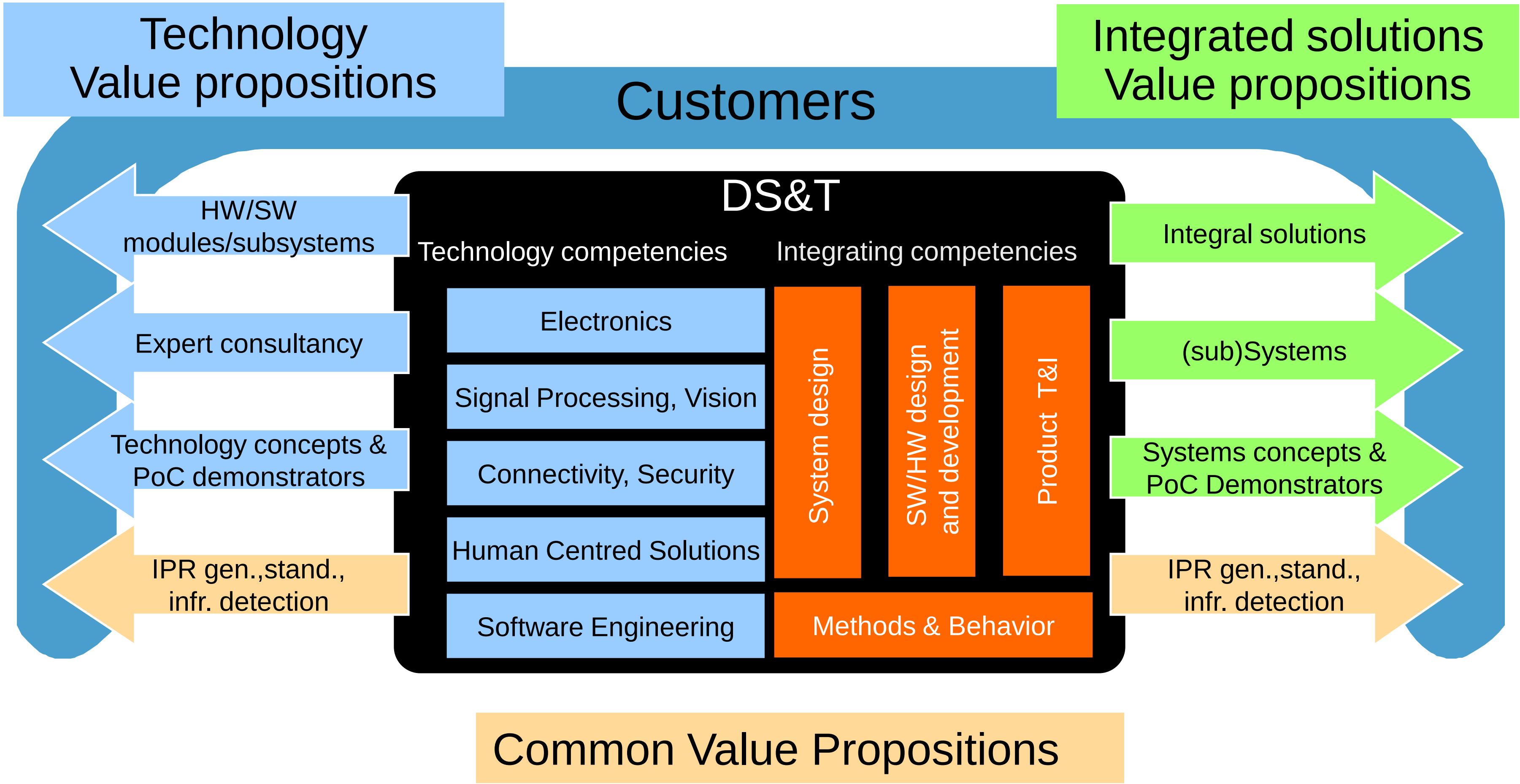
Digital Systems & Technologies

Digital Systems & Technologies focuses on system design and realization of first-of-a-kind ‘digital technology based’ products.

Our technology base is geared around electronics, video, imaging & vision, human centered design, audio processing, security/digital rights management and connectivity.

PHILIPS

DS&T - Technologies and Integral Solutions



Technology Value propositions

Customers

Integrated solutions Value propositions

DS&T

Technology competencies

- Electronics
- Signal Processing, Vision
- Connectivity, Security
- Human Centred Solutions
- Software Engineering

Integrating competencies

- System design
- SW/HW design and development
- Product T&I
- Methods & Behavior

- HW/SW modules/subsystems
- Expert consultancy
- Technology concepts & PoC demonstrators
- IPR gen.,stand., infr. detection

- Integral solutions
- (sub)Systems
- Systems concepts & PoC Demonstrators
- IPR gen.,stand., infr. detection

Common Value Propositions

Security

What is security?

Protection against loss

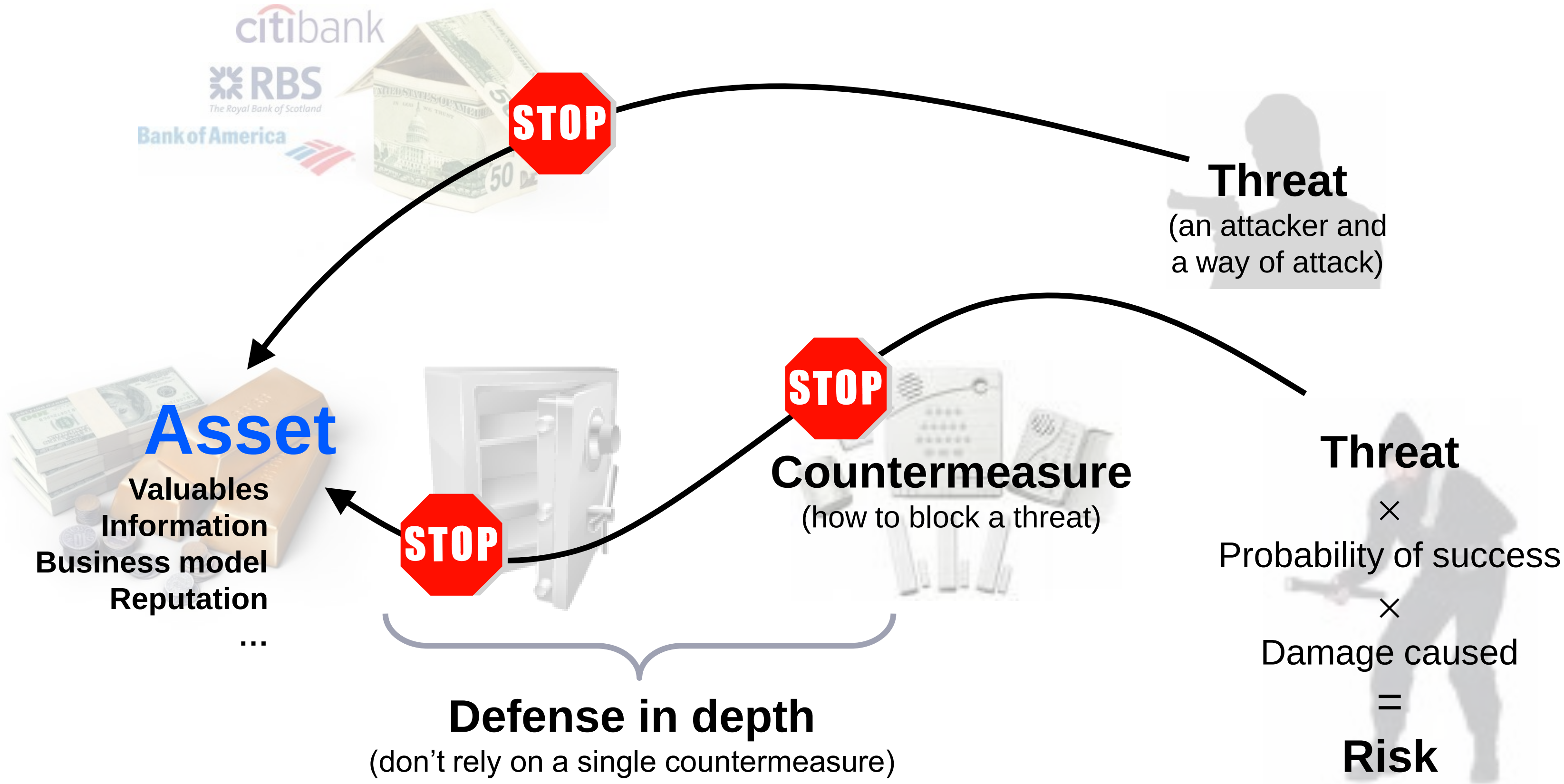
due to intentional actions from others

Security

due to failures/accidents

Safety

Security is not a product: it is a process



Threat
(an attacker and
a way of attack)

Asset

Valuables
Information
Business model
Reputation
…

Countermeasure
(how to block a threat)

Threat
×
Probability of success
×
Damage caused
=
Risk

Defense in depth
(don't rely on a single countermeasure)

Trade-off: is the risk sufficiently high to warrant the countermeasure(s)?

PHILIPS

Security is everywhere

At Home

Seals & tamper-resistant / evident packaging

Home automation system

Utilities metering

Burglar alarm

Door locks & bolts

Safe

WLAN

Dog

e-Book

Pay-TV

DVD / Blu-ray Disc

Game console

Health monitoring system

At Work

Ink cartridges

Firewall

Computer network login

Secured web session

Antivirus

Password management

Intrusion detection system

Access control

Company badge

Guards

Financial audit

Doing Leisure / Sports

Pay-TV (Hotel)

Building automation system

Ticket

Training data aggregation

On the Road

Passport

Airport Security

Biometric identification

In-flight entertainment

Portable media player

Ticket (OV chip card)

Cell phone

Car alarm

Toll road

TPMS

Inter-car Control Systems

Navigation (maps)

When Shopping

Automated product scanning

Theft prevention

Security camera

Building automation system

Payment system

Customer loyalty program

At the doctor’s

Asset / people tracking

HIPAA / European directive

Electronic medical records

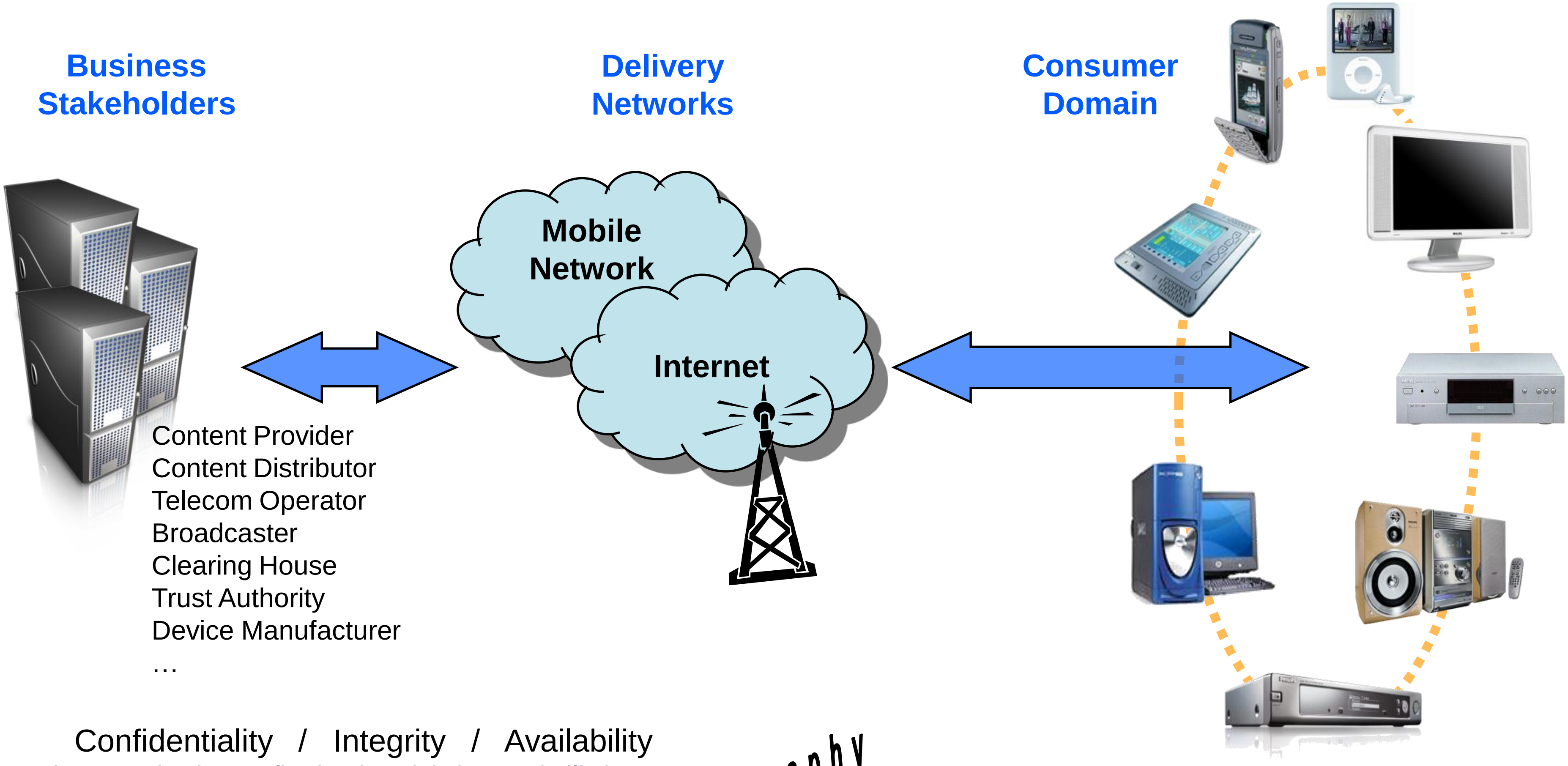
Bedside patient monitoring

Implants e.g. pacemaker

Medical data communication

What is our background?

A decade of Digital Rights Management / Copy Protection / Conditional Access



Business Stakeholders

Delivery Networks

Consumer Domain

Content Provider
Content Distributor
Telecom Operator
Broadcaster
Clearing House
Trust Authority
Device Manufacturer
…

Confidentiality / Integrity / Availability
(possession/control) (authenticity) (utility)

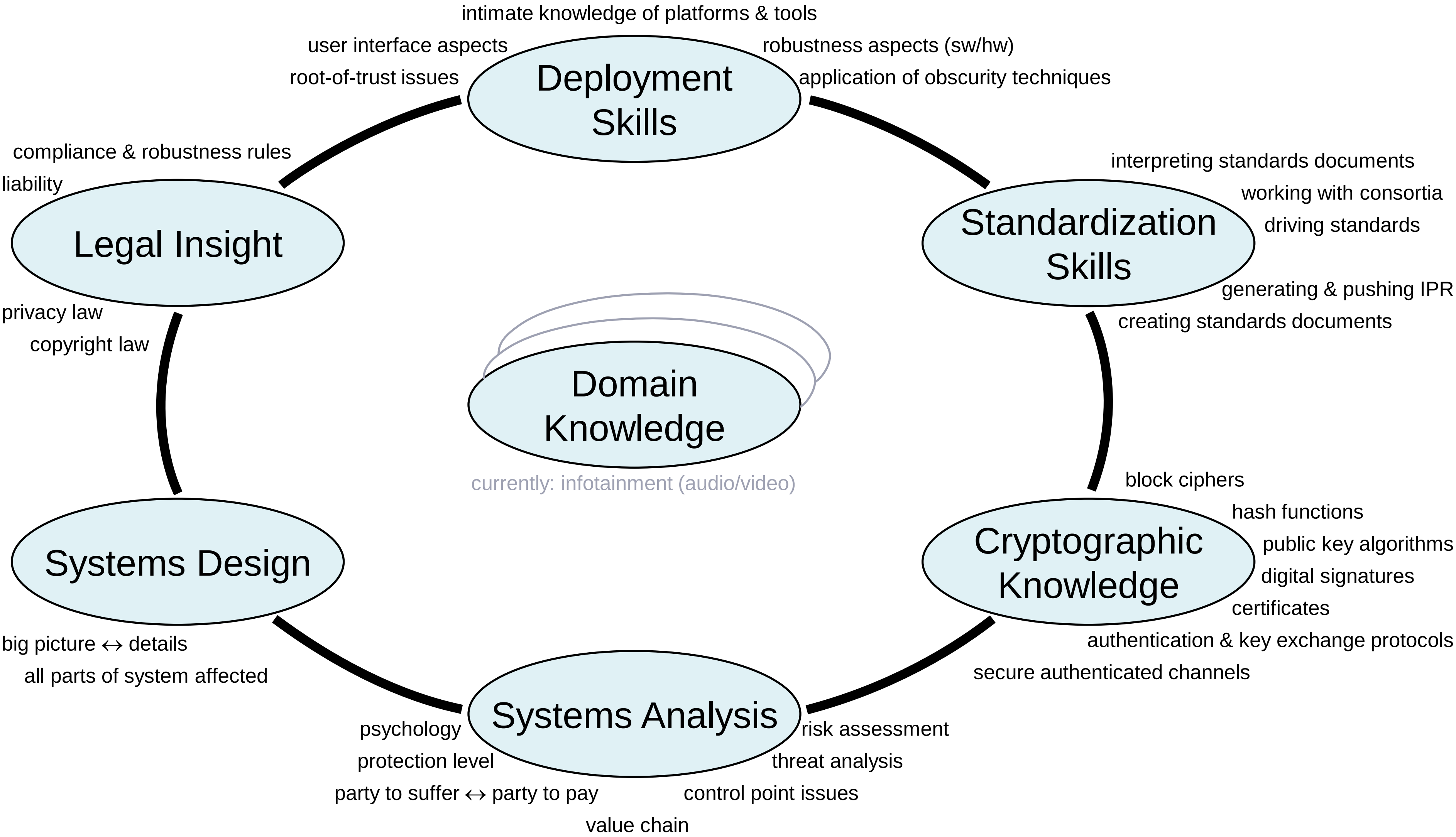
cryptography

Identification / Authentication / Authorization
(who are you?) (prove it) (you can do this)

Challenges when selling security

- Security often involves conflict of interests
  - Party to protect a system ≠ party to suffer from security failure
  - Party to paying for security ≠ party to profit from security
    - Infotainment: player manufacturer ↔ content owner ↔ consumer
    - Medical: insurance ↔ care organization ↔ patient
    - Financial: bank ↔ end customer
- Security is (only) applied because of regulations / contracts
- Security often is added as an afterthought
- Security may be used to achieve vendor lock-in
- Security is (almost) always regarded as a hassle
  - Unavoidable because of trade-offs involved

Competences of a security expert



The Technology Landscape

Basic Technology Components

Examples for Information Security

Cryptographic functions	• Block Ciphers	AES, DES, …
	• One-way Hash Functions	SHA-256, MD5, …
	• Public Key Algorithms / Digital signatures	RSA, ECC, DSA, …
	• White-box Crypto	(in research)

Cryptographic protocols	• Authentication & Key Exchange	DH, ISO 11770, …
	• Secure Authenticated Channel	SSL, TLS, …
	• Zero-knowledge Proof	
	• Multi-party Computation	(*e*-voting; in research)

Identification means	• Unique Identifiers / Certificates	anti-counterfeiting
	• Physically Unclonable Functions / “Dongles”	
	• Biometric Properties	
	• Fingerprints / Watermarks	

Basic Technology Components

Examples for Information Security

Software engineering

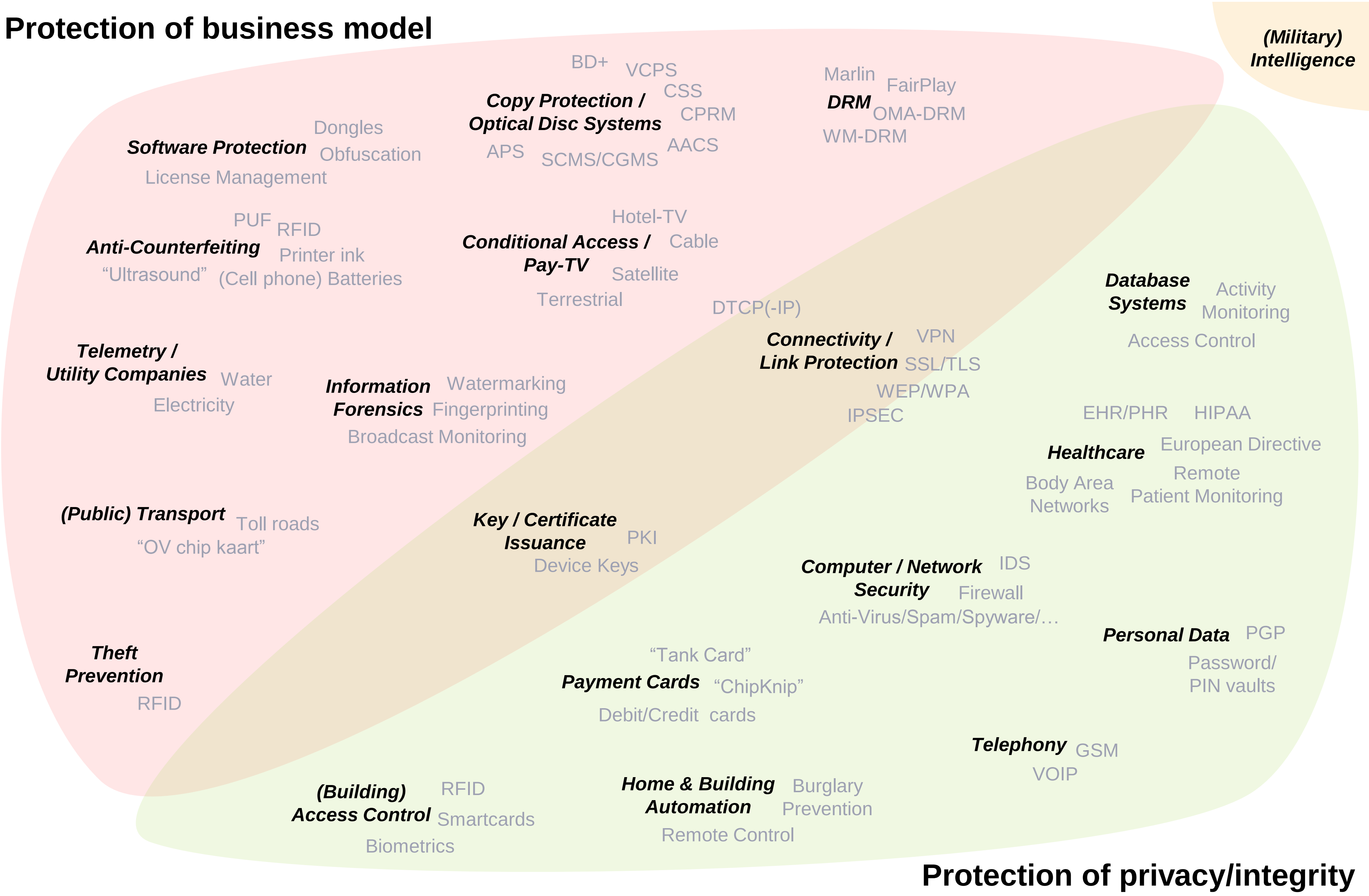
- Code Review & Bug Elimination
- Mandatory Access Controls (minimize damage in case of security breach)
- Micro Kernels / Reduction of the Trusted Code Base
- Code Obfuscation / Tamper Resistance

Hardware support

- Smart Cards
- Separate (Embedded) Security Processors / TPM
- TrustZone (ARM)
- Virtualization Support

Policy

- Access Control / Systems Isolation
- Event Logging & Log Inspection / Intrusion Detection
- Security Auditing / Common Criteria
- Trust Management / Authorization Control



Protection of business model

(Military) Intelligence

Software Protection
Dongles
Obfuscation
License Management

Copy Protection / Optical Disc Systems
BD+
VCPS
CSS
CPRM
AACS
APS
SCMS/CGMS

DRM
Marlin
FairPlay
OMA-DRM
WM-DRM

Anti-Counterfeiting
PUF
RFID
Printer ink
"Ultrasound"
(Cell phone) Batteries

Conditional Access / Pay-TV
Hotel-TV
Cable
Satellite
Terrestrial

DTCP(-IP)

Database Systems
Activity Monitoring
Access Control

Telemetry / Utility Companies
Water
Electricity

Information Forensics
Watermarking
Fingerprinting
Broadcast Monitoring

Connectivity / Link Protection
VPN
SSL/TLS
WEP/WPA
IPSEC

Healthcare
EHR/PHR
HIPAA
European Directive
Remote Patient Monitoring
Body Area Networks

(Public) Transport
Toll roads
"OV chip kaart"

Key / Certificate Issuance
PKI
Device Keys

Computer / Network Security
IDS
Firewall
Anti-Virus/Spam/Spyware/…

Personal Data
PGP
Password/ PIN vaults

Theft Prevention
RFID

Payment Cards
"Tank Card"
"ChipKnip"
Debit/Credit cards

Telephony
GSM
VOIP

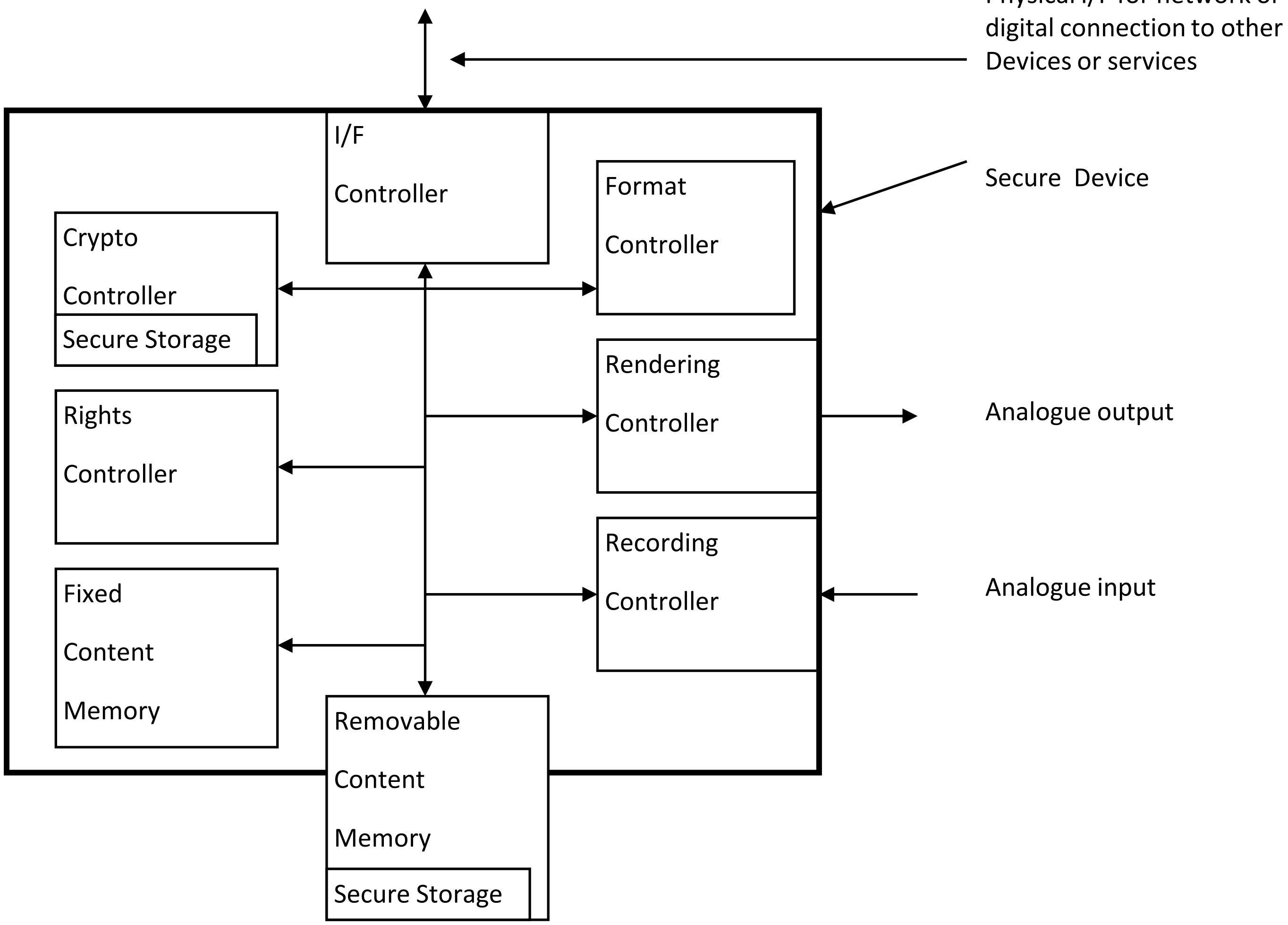
(Building) Access Control
RFID
Smartcards
Biometrics

Home & Building Automation
Burglary Prevention
Remote Control

Protection of privacy/integrity

Example: Hard-Disk / DVD Recorder

Block diagram of a Secure Device



Examples of threats (1)

- Unauthorized disclosure of clear content
  - Unauthorized rendering
  - Unauthorized export
  - Tampering

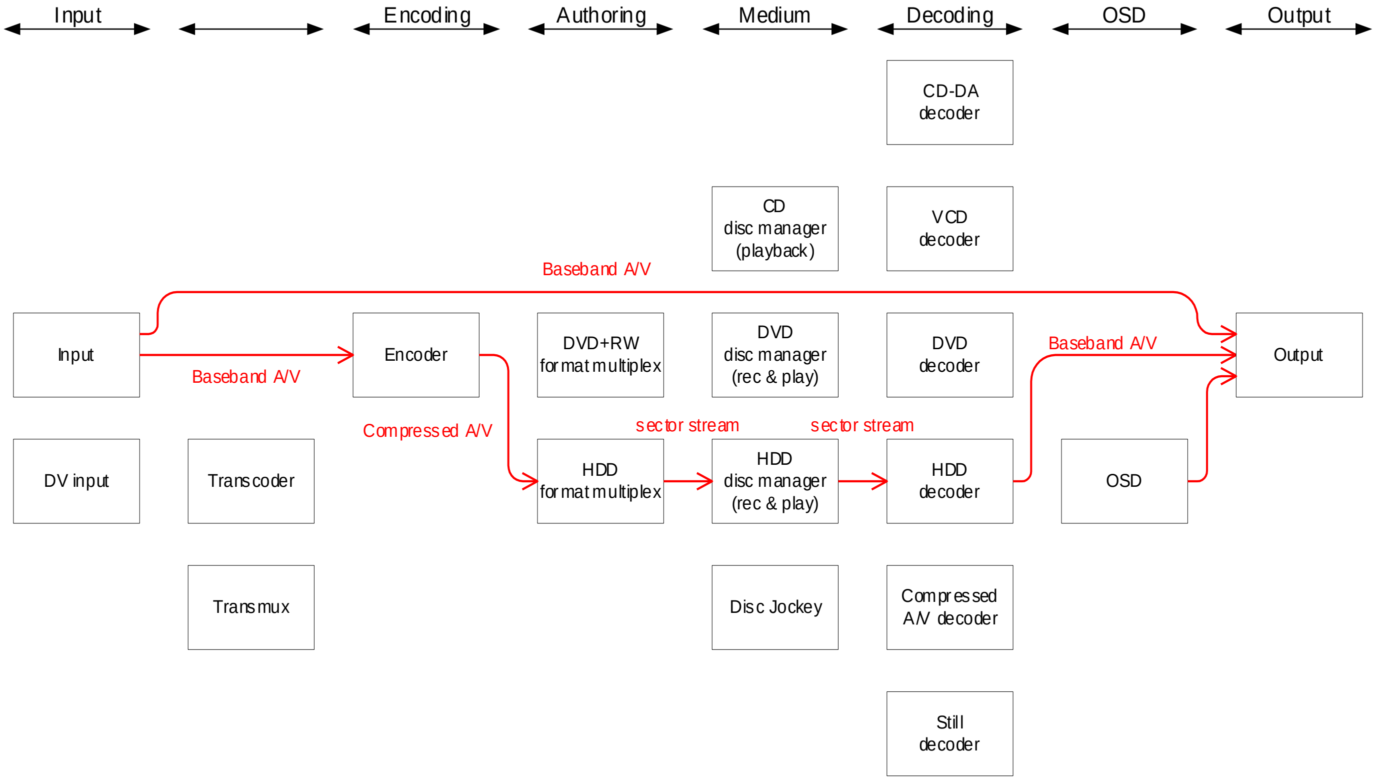
APS, CGMS

encrypted internal comm

- Unauthorized modification of clear content
  - Analog inputs/outputs
  - Tampering

PHILIPS

Data paths



Philips Applied Technologies

Examples of threats (2)

- Misuse of target
  - Import of impersonated content — software upgrade
  - Unauthorized export
  - Import & rendering of unauthorized content — CSS, region code

- Other threats
  - Cloning the target
  - Unauthorized disclosure of firmware
  - License disclosure/modification
  - Key disclosure/modification — CSS
  - Rights modification — make region free

More than a decade of content protection @Apptech

Marlin

a DRM system for CE
standardization & implementation
server & multi-device demo

Pit-O-Resc

a tamper-resistant LBR controller platform
secure handling of keys & algorithms

WM-DRM

consultancy on Compliance & Robustness rules,
and its industrialization within a CE environment

Modena

implementation of PC-client, server
& rights issuer for OMA DRM

DVD-Video

implementation of CSS,
the copy protection system of DVD

Long Pura

DRM in a distributed environment
standardization & implementation

OMA B-cast / DCB SPP & IEC 62455

“open” protection standard for
digital broadcast (IP & MPEG TS)

Key Issuance Tools

database of cryptographic keys
for various protection systems
implementation & deployment

CD2/DMX

a DRM/CP system for CD, including
an Electronic Music Download system

Sapphire

a DRM/CP system integrated
in an optical disc drive

DVB CI+

driving the standardization process,
defining & implementing the specification

Blu-ray Disc

consultancy on AACS/BD+/ROM Mark
copy protection features; implementation

Super Audio CD

implementation of a ROM Mark detector
and the copy protection system

Millennium Watermark

a hardware implementation
of a video watermark detector

PHILIPS

sense and simplicity