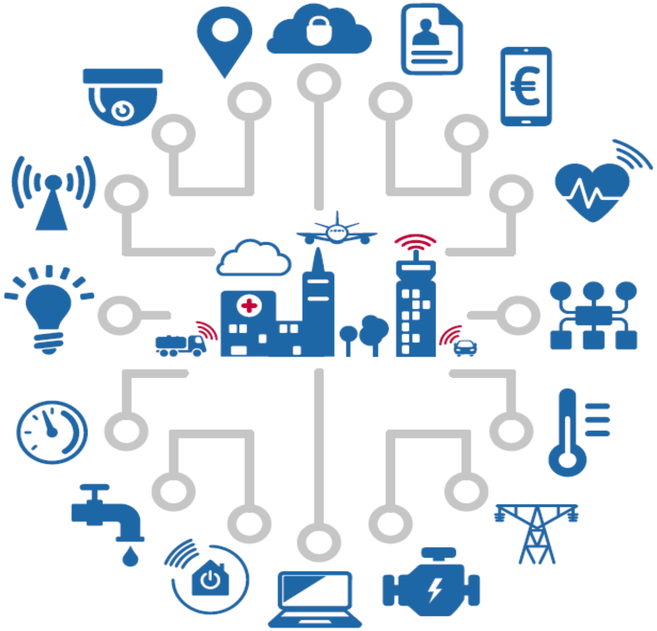
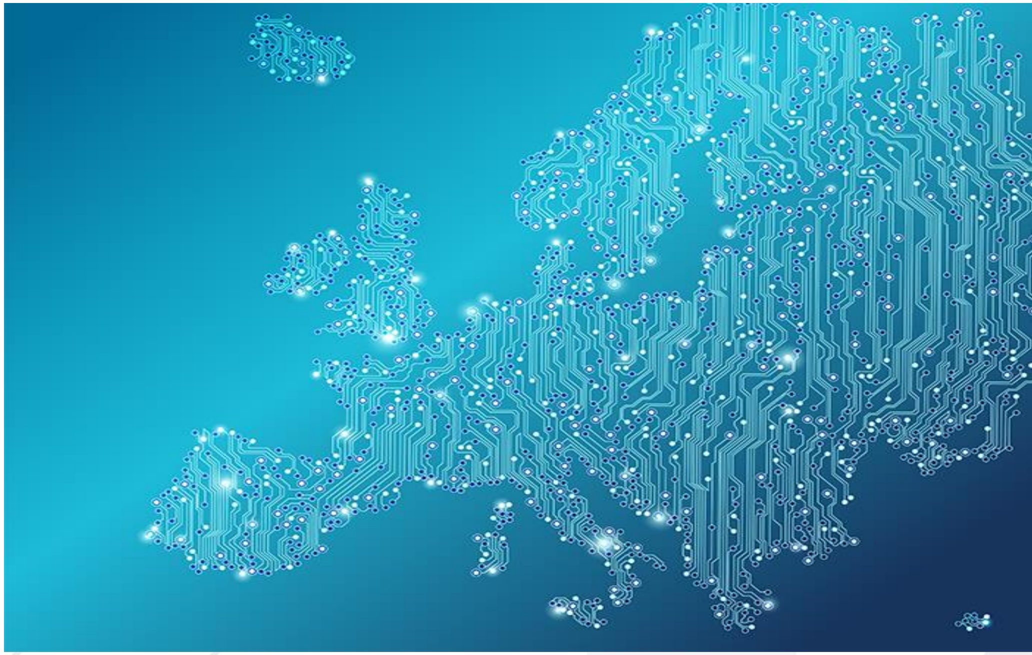




Trusted IoT Strategies for the future: ENISA's efforts to foster IoT cybersecurity

Dr Fabio Di Franco

IOT week| Bilbao| 07.06.2018

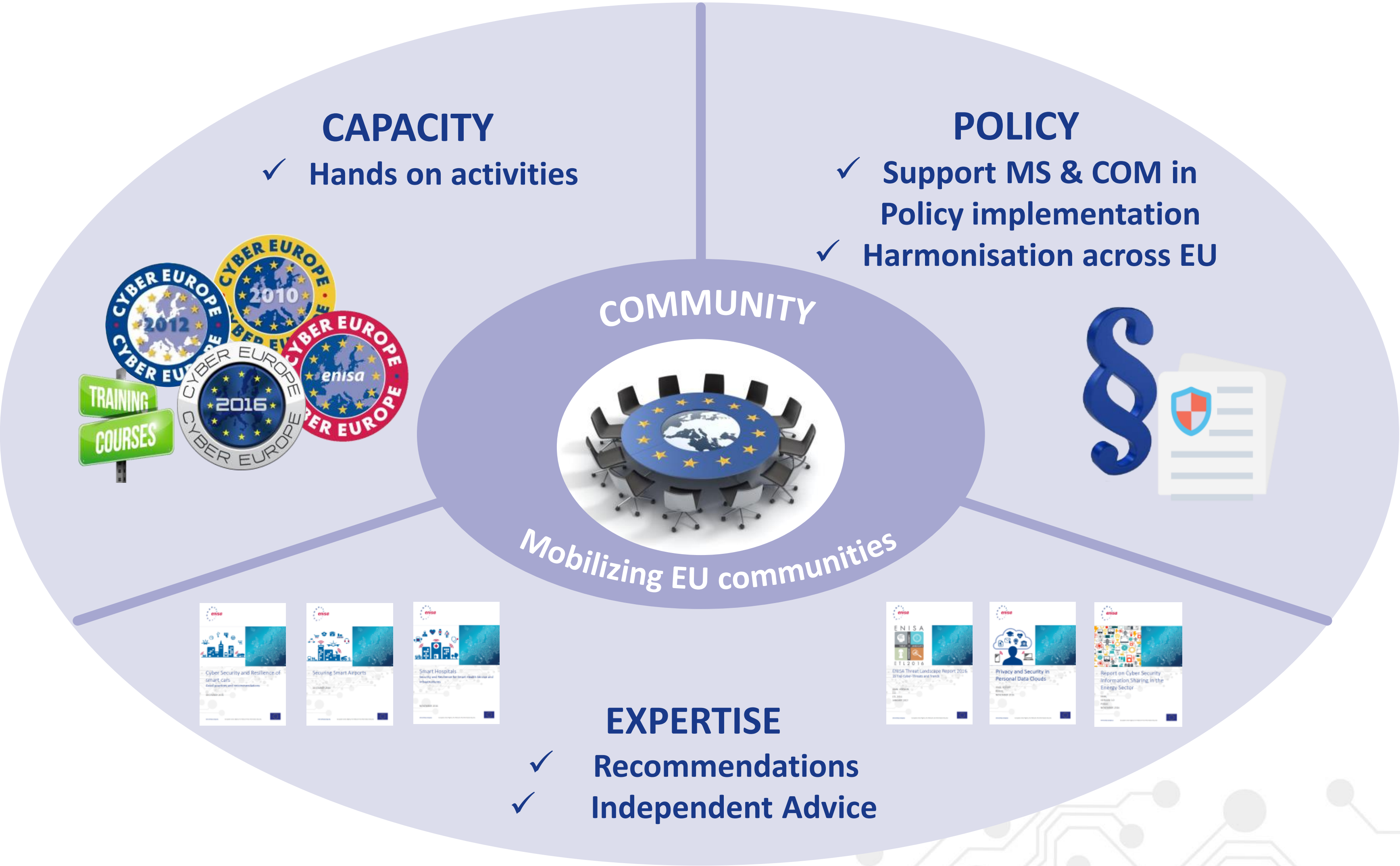
European Union Agency for Network and Information Security (ENISA)

Securing Europe’s Information Society

Operational Office in Athens

Seat in Heraklion

Positioning ENISA activities


CYBER EUROPE 2010
CYBER EUROPE 2012
CYBER EUROPE 2016
CYBER EUROPE enisa
TRAINING COURSES
§
Cyber Security and Resilience of smart cars
Securing Smart Airports
Smart Hospitals
ENISA Threat Landscape Report 2016
Privacy and Security in Personal Data Clouds
Report on Cyber Security Information Sharing in the Energy Sector

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

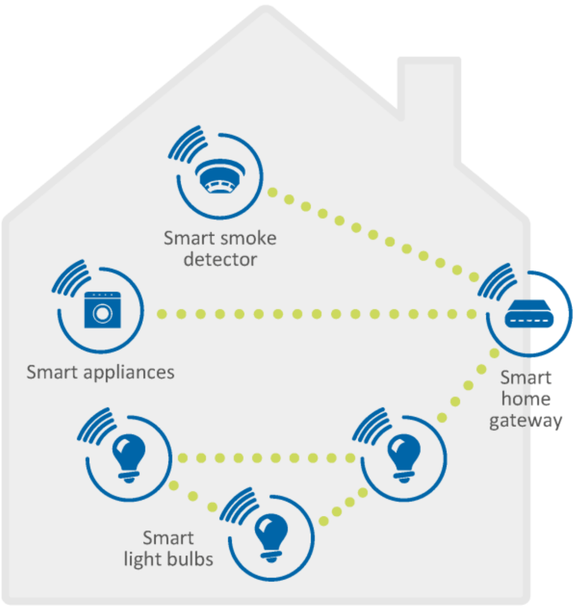
COMMUNITY

Mobilizing EU communities

EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

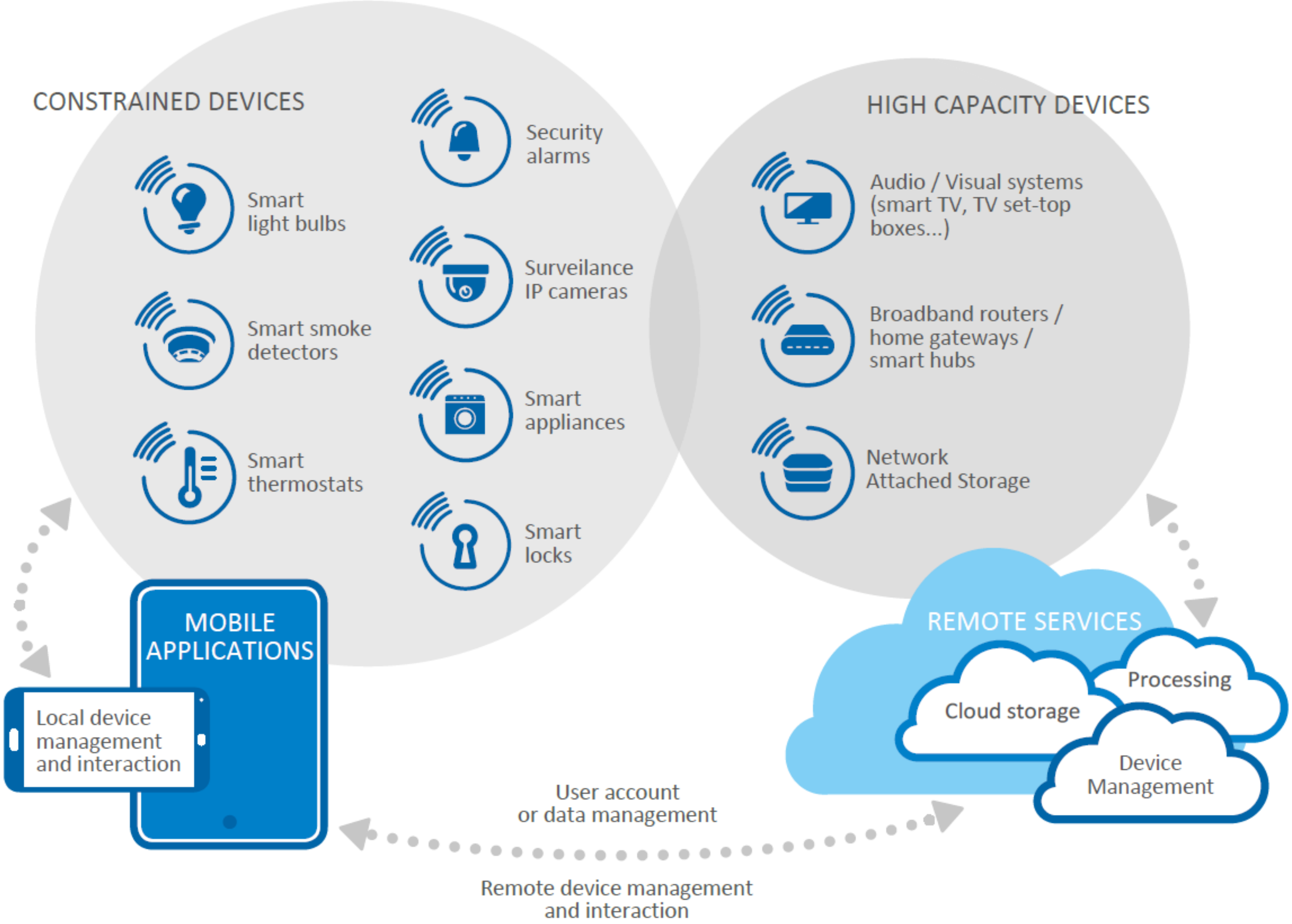
Security Considerations in IoT



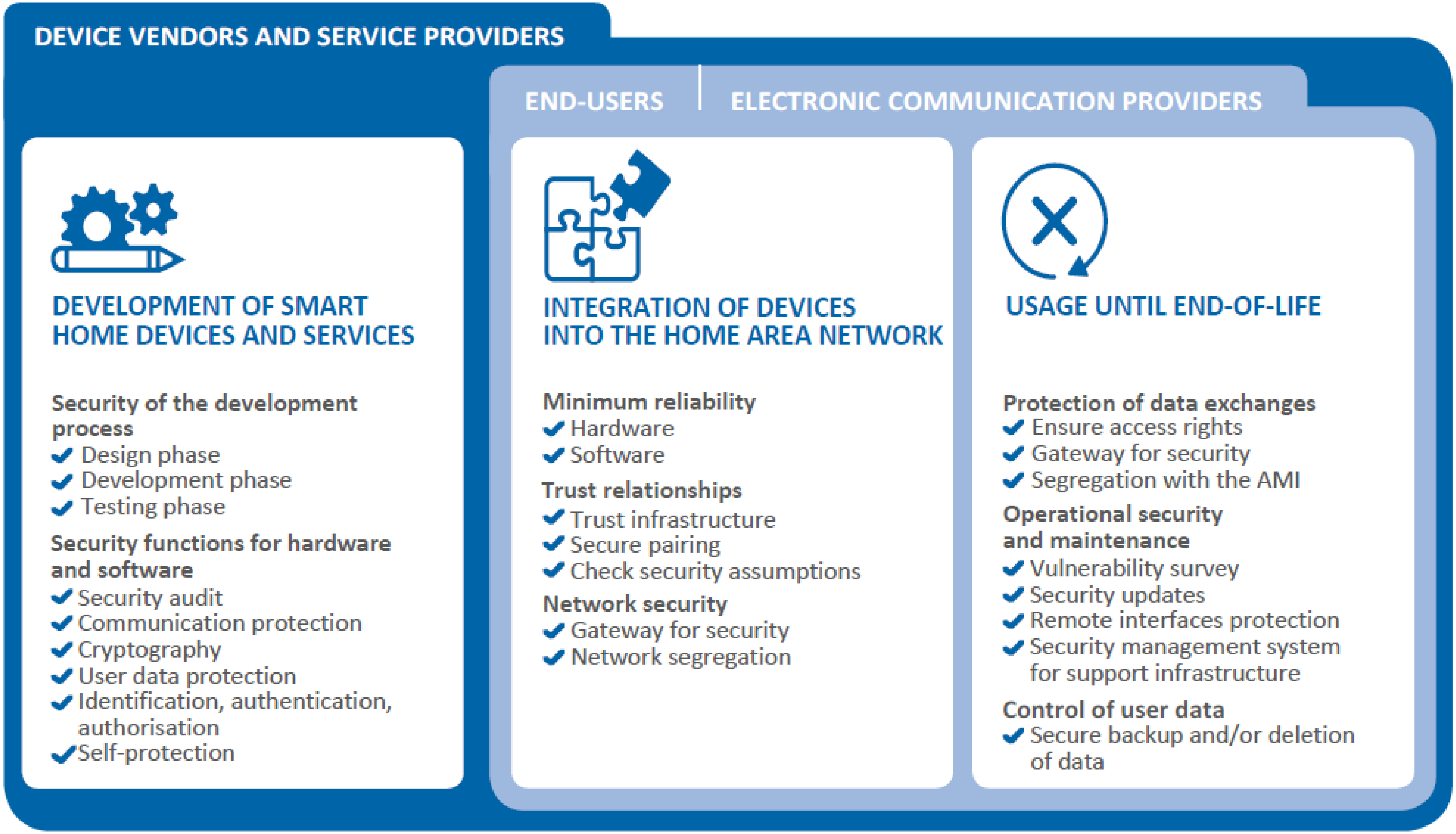
- Very large attack surface: the threat landscape concerning IoT is extremely wide.
- Complex ecosystem: involving aspects such as devices, communications, interfaces, and people.
- Security integration: legacy products might not guarantee any security
- Difficult to secure the entire lifecycle of products
- Fragmentation of the standards and regulations
- Insecure programming and reuse of unsecure/deprecated code
- Unclear liabilities
- Limited device resources
- Security is not yet a market differentiator.

Sources: Baseline Security Recommendations for IoT – ENISA
Security and Resilience of Smart Home Environments - ENISA

Smart Home


CONSTRAINED DEVICES
Smart light bulbs
Smart smoke detectors
Smart thermostats
Security alarms
Surveilance IP cameras
Smart appliances
Smart locks
HIGH CAPACITY DEVICES
Audio / Visual systems (smart TV, TV set-top boxes...)
Broadband routers / home gateways / smart hubs
Network Attached Storage
MOBILE APPLICATIONS
Local device management and interaction
REMOTE SERVICES
Processing
Cloud storage
Device Management
User account or data management
Remote device management and interaction

Good practices within the Smart Home lifecycle and their applicability to stakeholders



DEVICE VENDORS AND SERVICE PROVIDERS

END-USERS | ELECTRONIC COMMUNICATION PROVIDERS

DEVELOPMENT OF SMART HOME DEVICES AND SERVICES

Security of the development process

- ✓ Design phase
- ✓ Development phase
- ✓ Testing phase

Security functions for hardware and software

- ✓ Security audit
- ✓ Communication protection
- ✓ Cryptography
- ✓ User data protection
- ✓ Identification, authentication, authorisation
- ✓ Self-protection

INTEGRATION OF DEVICES INTO THE HOME AREA NETWORK

Minimum reliability

- ✓ Hardware
- ✓ Software

Trust relationships

- ✓ Trust infrastructure
- ✓ Secure pairing
- ✓ Check security assumptions

Network security

- ✓ Gateway for security
- ✓ Network segregation

USAGE UNTIL END-OF-LIFE

Protection of data exchanges

- ✓ Ensure access rights
- ✓ Gateway for security
- ✓ Segregation with the AMI

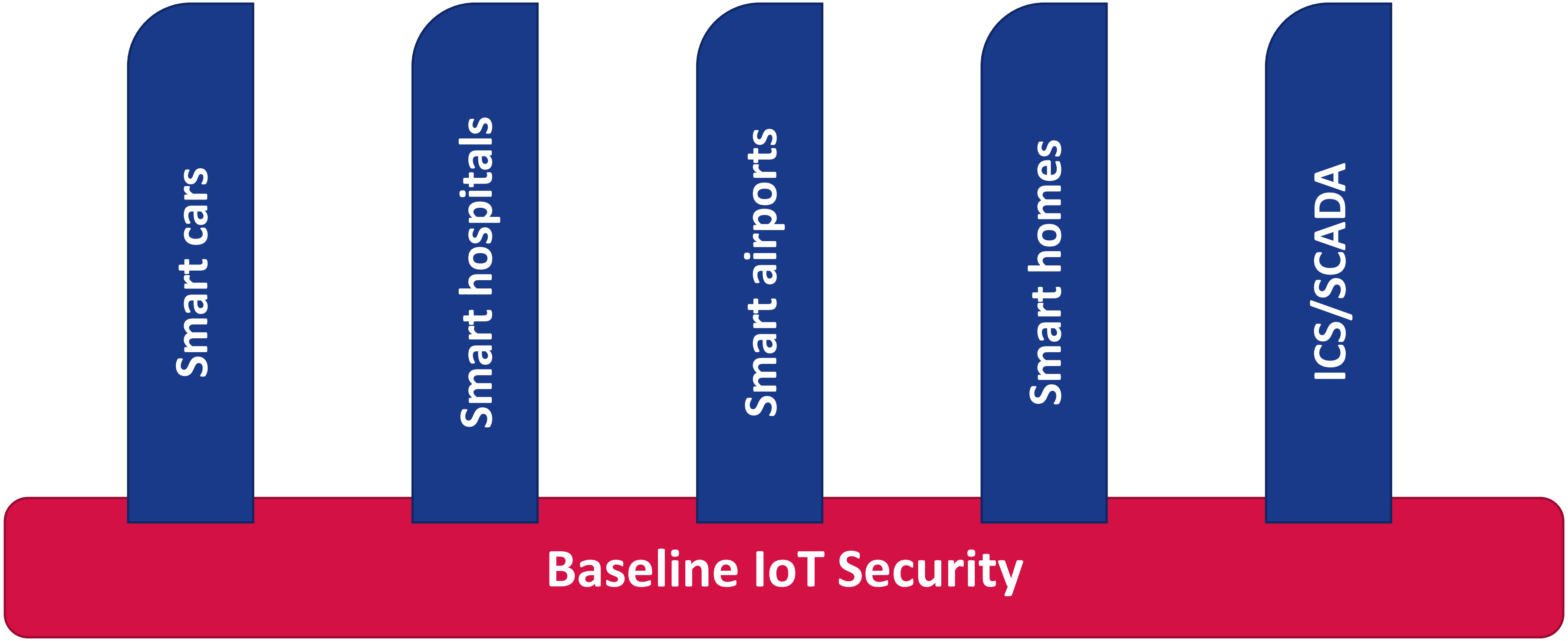
Operational security and maintenance

- ✓ Vulnerability survey
- ✓ Security updates
- ✓ Remote interfaces protection
- ✓ Security management system for support infrastructure

Control of user data

- ✓ Secure backup and/or deletion of data

How do we secure IoT?



Smart cars

Smart hospitals

Smart airports

Smart homes

ICS/SCADA

Baseline IoT Security

IoT Security Measures

Policies

- Security by design
- Privacy by design
- Asset Management
- Risk and Threat Identification and Assessment

Organizational, People and Processes

- End-of-life support
- Proven solutions
- Management of security vulnerabilities and/or incidents
- Human Resources Security Training and Awareness
- Third-Party relationships

Technical

- Hardware security
- Trust and Integrity Management
- Strong default security and privacy
- Data protection and compliance
- System safety and reliability
- Secure Software / Firmware updates
- Authentication
- Authorization
- Access Control - Physical and Environmental security
- Cryptography
- Secure and trusted communications
- Secure Interfaces & network services
- Secure input and output handling
- Logging
- Monitoring and Auditing

Baseline IoT Security Recommendations

- Promote **harmonization of IoT security initiatives** and regulations
- **Raise awareness** of the need for IoT cybersecurity
- Define **secure software and hardware development lifecycle guidelines** for IoT
- Achieve **consensus on interoperability** across the IoT ecosystem
- Foster **economic and administrative incentives** for IoT security
- Establish **secure IoT product/service lifecycle management**
- Clarify **liability** among IoT stakeholders

https://enisa.europa.eu/iot

Future steps for IoT Security

- Essential to consider and ensure IoT security in all stages of the life cycle of products and services
  - Design, development, testing, usage, maintenance (security updates) and decommissioning
- Establish baseline security measures for IoT across sectors
  - Such measures will form the basis to evaluate/assess relevant products & services
- Raise awareness on IoT security (threats, risks, solutions)
  - Involve all stakeholders since it is a multi-faceted issue
  - Consumers to play a focal role (updates, awareness)

enisa

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu

INTERNET OF THINGS
SECURITY CONFERENCE

Europol - ENISA 24-25 October 2018