GDPR IN THE IOT: REDUCING FINANCIAL RISKS BY DEFINING STANDARDS ON ‘TECHNICAL MEASURES’ REQUIRED BY ARTICLE 25 & 32

JACQUES KRUSE BRANDAO
ENISA-CEN-CSCG WORKSHOP
19 SEPTEMBER 2017

BRUSSELS

EXTERNAL USE

Article 32 GDPR

- …. controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and **encryption of personal data**;

(b) the ability to **ensure** the ongoing **confidentiality**, **integrity**, **availability** and **resilience of processing systems and services**;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 25 GDPR

- Taking into account the state of the art, the cost of implementation and the nature, scope, (…) the controller shall, (…), implement appropriate technical and organisational measures, such as pseudonymisation, (…), such as data minimization, (…)

Problem

1. What are appropriate technical measures?
2. What is “State-of-the-Art”?

- ➢ Up to now there is no technical catalogue or guideline available what exactly needs to be implemented in terms of cybersecurity into IoT devices which are processing (handling, using, storing, deleting, etc.) personal data to fulfil the GDPR requirements.
- ➢ Standards do only exist for specific segments and use cases.
- ➢ State of the art is dynamic.
- ➢ Fast innovation cycles make it difficult for standardization to be on time.
- ➢ “Security” is mentioned 50 x in GDPR text. But not defined in detail.

-> This leads to uncertainty among industry.

What do we need?

- Generate Legal certainty for investors by defining “certification of privacy”
- Enhance the European Cybersecurity Certification Framework
  by privacy requirements to fill the requirements of the GDPR,
  involving the EDPB and national data protection authorities
- “Impact”:
  Generate Risk+Impact Assessment Framework,
  e.g. higher security levels for more sensitive data (e.g. patients file vs. fridge content)

- “State-of-the-Art”: Generate Catalogue of key principles for security and privacy,
  based on existing standards, e.g. privacy features in SMGW / Comms Hubs / etc.
- A mapping of each key principle to existing standard(s) and certification schemes
- Filling the gaps via ESO

Technology has outstripped our Security & Safety Legal & Standard Framework

- Law Firm *Arthur’s Legal* has analyzed 27 SOTA Security Recommendations, Frameworks & Guidelines

Security in IoT / State of the Art (SOTA)

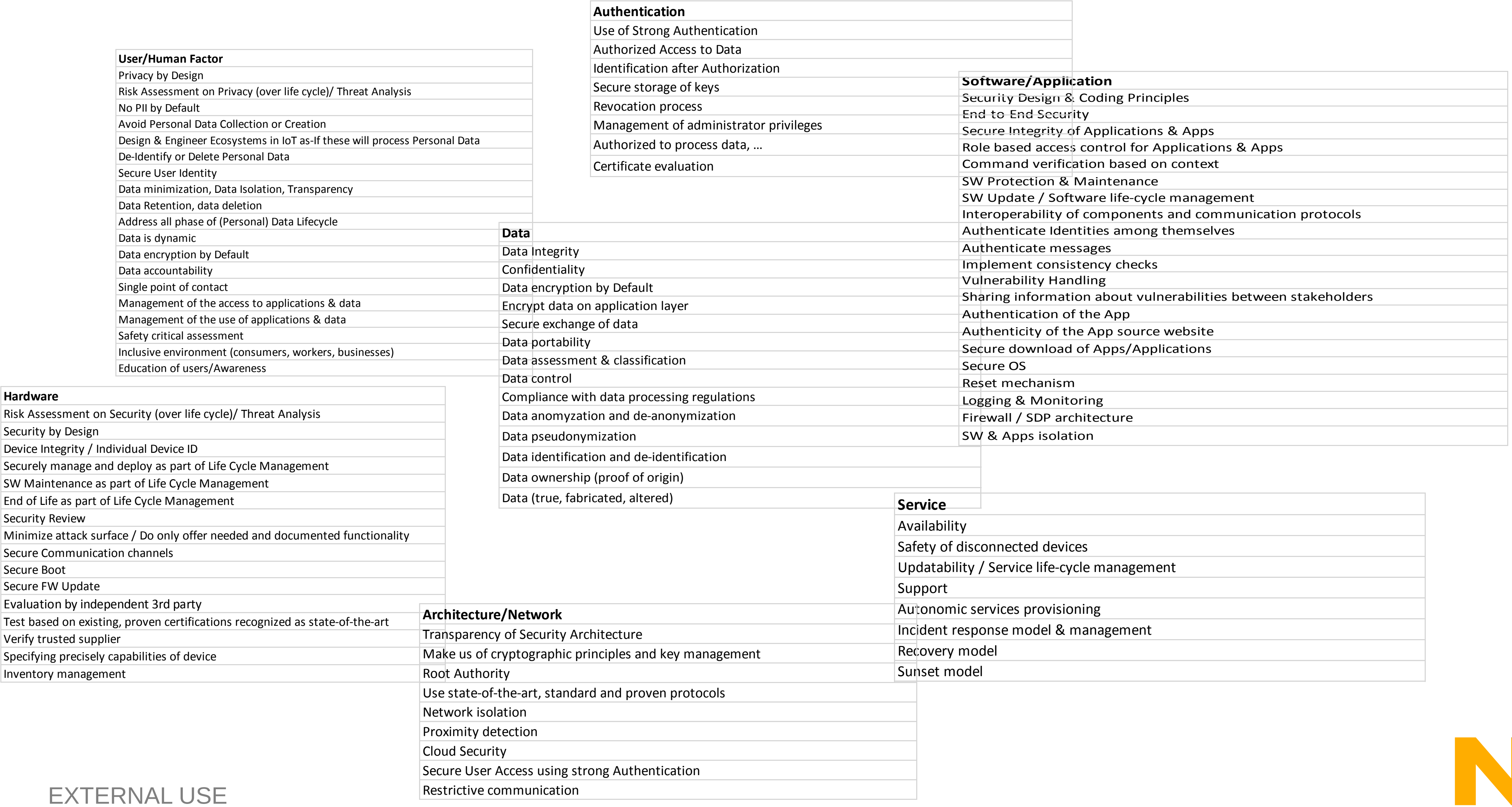
1. European Commission (EC) & Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security & Privacy in IoT (2017)
2. Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security and Privacy in the Hyper-Connected World (2016)
3. European Commission (EC): Best available techniques reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems (2016)
4. European Union Agency for Network and Information Security (ENISA): Auditing Security Measures (2013)
5. European Union Agency for Network and Information Security (ENISA): Cloud Certification Schemes Metaframework (2014)
6. Energy Expert Cyber Security Platform: Cyber Security in the Energy Sector (2017)
7. HM Government, Department for Transport and Centre for the Protection of National Infrastructure: The Key Principles of Cyber Security for Connected and Automated Vehicles (2017)
8. Autorité de régulation des communications électroniques et des postes (ARCEP): Preparing for the internet of things revolution (2016)
9. United States Department of Commerce (DoC): Fostering the advancement of the Internet of Things (2017)
10. United States Department of Homeland Security: Strategic Principles for Securing the Internet of Things (2016)
11. United States Department of Health and Human Services, Food and Drug Administration: Postmarket Management of Cybersecurity in Medical Devices (2016)
12. United States Department of Health and Human Services, Food and Drug Administration: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
13. United States Government Accountability Office: Technology Assessment: Internet of Things – Status and implications of an increasingly connected world (2017)
14. National Institute of Standards and Technology (NIST): Networks of ‘Things’ (2016)
15. IoT Alliance Australia (IoTAA): Internet of Things Security Guideline (2017)
16. GSM Association (GSMA): IoT Security Guidelines Overview Document (2016)
17. GSM Association (GSMA): IoT Security Guidelines for Service Ecosystems (2016)
18. GSM Association (GSMA): IoT Security Guidelines for Endpoint Ecosystems (2016)
19. GSM Association (GSMA): IoT Security Guidelines for Network Operators (2016)
20. IoT Security Foundation (IoTSF): IoT Security Compliance Framework (2016)
21. IoT Security Foundation (IoTSF): Connected Consumer Products Best Practice Guidelines (2016)
22. IoT Security Foundation (IoTSF): Vulnerability Disclosure (2016)
23. Broadband Internet Technical Advisory Group (BITAG): Internet of Things (IoT) Security and Privacy Recommendations (2016)
24. International Organization for Standardization (ISO): Internet of Things Preliminary Report (2014)
25. The Center for Internet Security (CIS): Critical Security Controls v6.0 (2016)
26. Internet Society: Global Internet Report 2016 (2016)
27. Tenable: Achieving Effective Cyber Hygiene (2016)

Technology has outstripped our Security & Safety Legal & Standard Framework

- Law Firm *Arthur’s Legal* has analyzed 27 SOTA Security Recommendations, Frameworks & Guidelines
- Segmentation of Requirements/Principles into 4 Layers & 3 Dimensions:
  - User/Human Factor
  - Data
  - Service
  - Software/Application
  - Hardware
  - Authentication
  - Infrastructure/Network

70+ Security Requirements & Principles could be derived from that exercise, e.g. end-to-end security, secure boot, secure storage of keys (see back-up)

Segmentation of Requirements/Principles



Authentication
Use of Strong Authentication
Authorized Access to Data
Identification after Authorization
Secure storage of keys
Revocation process
Management of administrator privileges
Authorized to process data, …
Certificate evaluation

User/Human Factor
Privacy by Design
Risk Assessment on Privacy (over life cycle)/ Threat Analysis
No PII by Default
Avoid Personal Data Collection or Creation
Design & Engineer Ecosystems in IoT as-If these will process Personal Data
De-Identify or Delete Personal Data
Secure User Identity
Data minimization, Data Isolation, Transparency
Data Retention, data deletion
Address all phase of (Personal) Data Lifecycle
Data is dynamic
Data encryption by Default
Data accountability
Single point of contact
Management of the access to applications & data
Management of the use of applications & data
Safety critical assessment
Inclusive environment (consumers, workers, businesses)
Education of users/Awareness

Software/Application
Security Design & Coding Principles
End to End Security
Secure Integrity of Applications & Apps
Role based access control for Applications & Apps
Command verification based on context
SW Protection & Maintenance
SW Update / Software life-cycle management
Interoperability of components and communication protocols
Authenticate Identities among themselves
Authenticate messages
Implement consistency checks
Vulnerability Handling
Sharing information about vulnerabilities between stakeholders
Authentication of the App
Authenticity of the App source website
Secure download of Apps/Applications
Secure OS
Reset mechanism
Logging & Monitoring
Firewall / SDP architecture
SW & Apps isolation

Data
Data Integrity
Confidentiality
Data encryption by Default
Encrypt data on application layer
Secure exchange of data
Data portability
Data assessment & classification
Data control
Compliance with data processing regulations
Data anomyzation and de-anonymization
Data pseudonymization
Data identification and de-identification
Data ownership (proof of origin)
Data (true, fabricated, altered)

Hardware
Risk Assessment on Security (over life cycle)/ Threat Analysis
Security by Design
Device Integrity / Individual Device ID
Securely manage and deploy as part of Life Cycle Management
SW Maintenance as part of Life Cycle Management
End of Life as part of Life Cycle Management
Security Review
Minimize attack surface / Do only offer needed and documented functionality
Secure Communication channels
Secure Boot
Secure FW Update
Evaluation by independent 3rd party
Test based on existing, proven certifications recognized as state-of-the-art
Verify trusted supplier
Specifying precisely capabilities of device
Inventory management

Service
Availability
Safety of disconnected devices
Updatability / Service life-cycle management
Support
Autonomic services provisioning
Incident response model & management
Recovery model
Sunset model

Architecture/Network
Transparency of Security Architecture
Make us of cryptographic principles and key management
Root Authority
Use state-of-the-art, standard and proven protocols
Network isolation
Proximity detection
Cloud Security
Secure User Access using strong Authentication
Restrictive communication

Technology has outstripped our Security & Safety Legal & Standard Framework

- Law Firm *Arthur's Legal* has analyzed 27 SOTA Security Recommendations, Frameworks & Guidelines (BITAG, GSMA, DoHS, EC&AIOTI, etc.)
- Segmentation of Requirements/Principles into 4 Layers & 3 Dimensions:
  - User/Human Factor
  - Data
  - Service
  - Software/Application
  - Hardware
  - Authentication
  - Infrastructure/Network

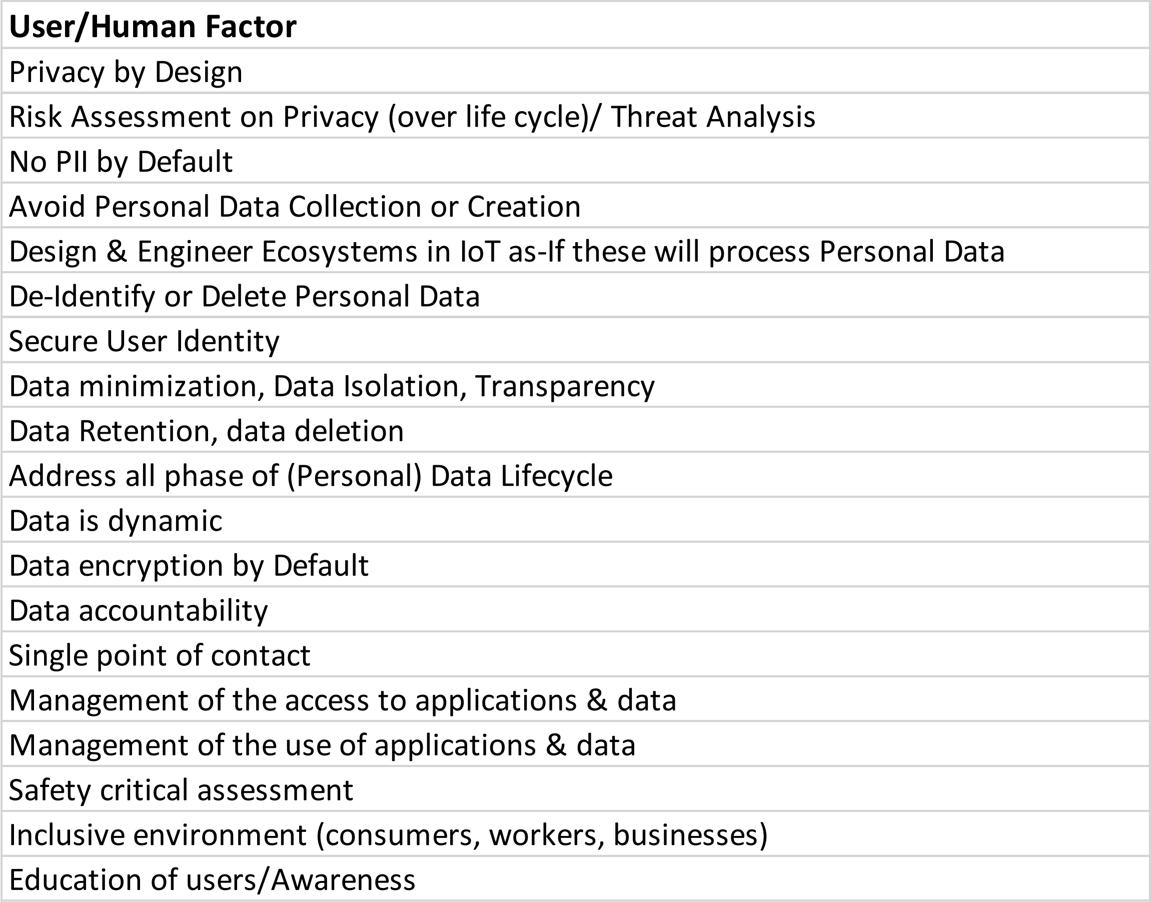
70+ Security Requirements & Principles could be derived from that exercise,
e.g. end-to-end security, secure boot, secure storage of keys (see back-up)

- Objective before May 25, 2018:
  Identifying and filling the gaps to generate a technical catalogue or guideline to get legal certainty not only for the backend systems but also for the planned 50B IoT devices expected by 2020

THANK YOU!

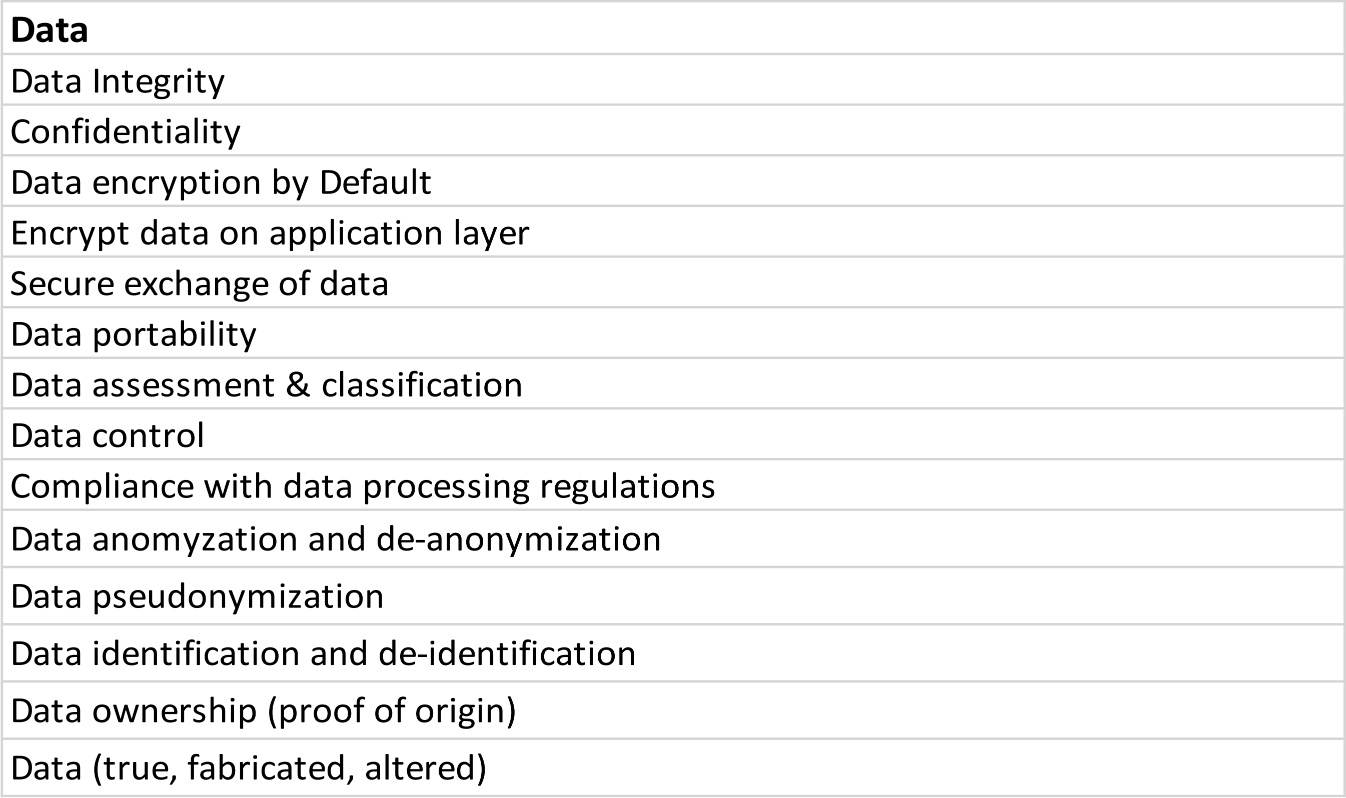
BACK-UP

User/Human Factor



User/Human Factor
Privacy by Design
Risk Assessment on Privacy (over life cycle)/ Threat Analysis
No PII by Default
Avoid Personal Data Collection or Creation
Design & Engineer Ecosystems in IoT as-If these will process Personal Data
De-Identify or Delete Personal Data
Secure User Identity
Data minimization, Data Isolation, Transparency
Data Retention, data deletion
Address all phase of (Personal) Data Lifecycle
Data is dynamic
Data encryption by Default
Data accountability
Single point of contact
Management of the access to applications & data
Management of the use of applications & data
Safety critical assessment
Inclusive environment (consumers, workers, businesses)
Education of users/Awareness

Data

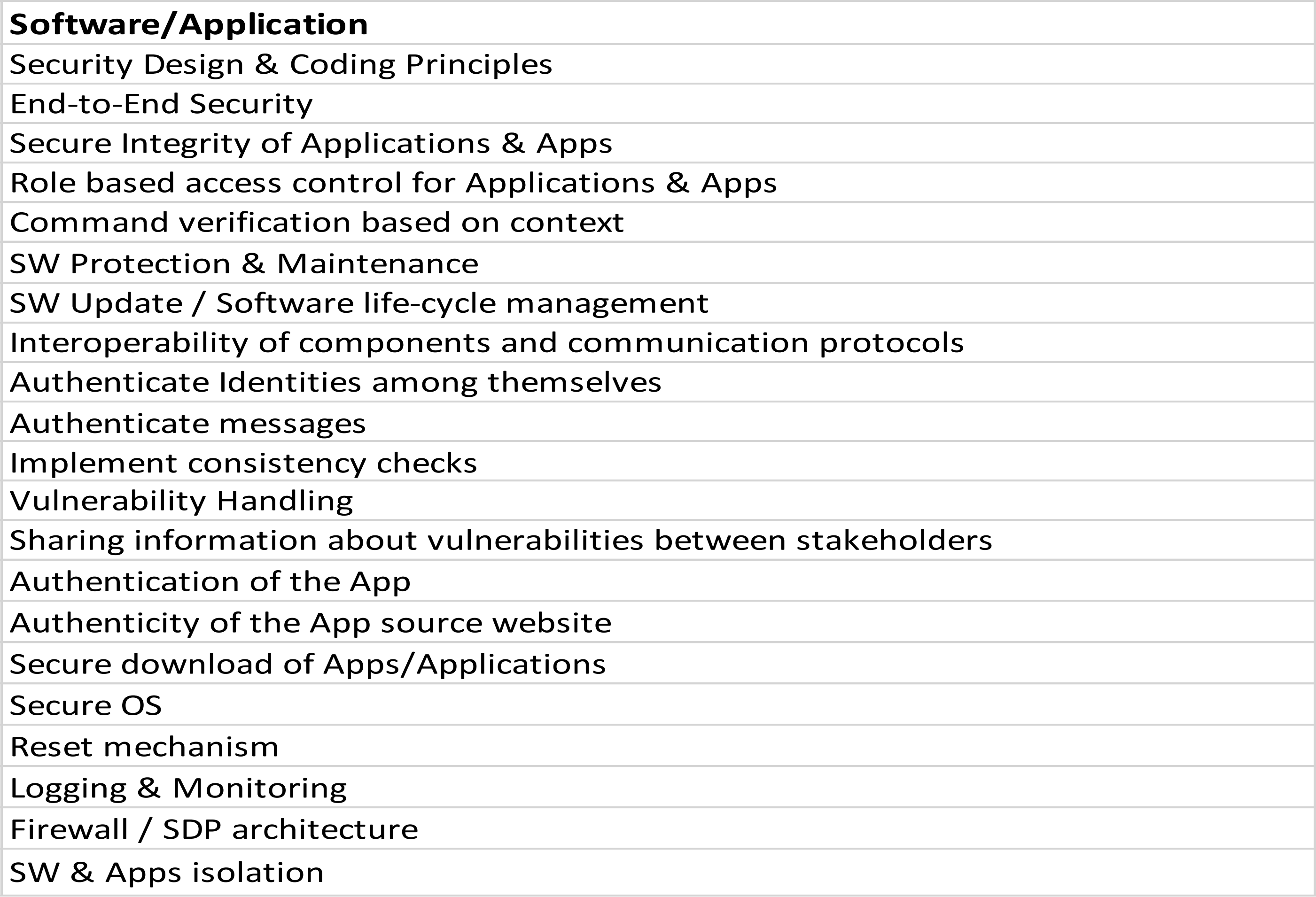


Data
Data Integrity
Confidentiality
Data encryption by Default
Encrypt data on application layer
Secure exchange of data
Data portability
Data assessment & classification
Data control
Compliance with data processing regulations
Data anomyzation and de-anonymization
Data pseudonymization
Data identification and de-identification
Data ownership (proof of origin)
Data (true, fabricated, altered)

Service

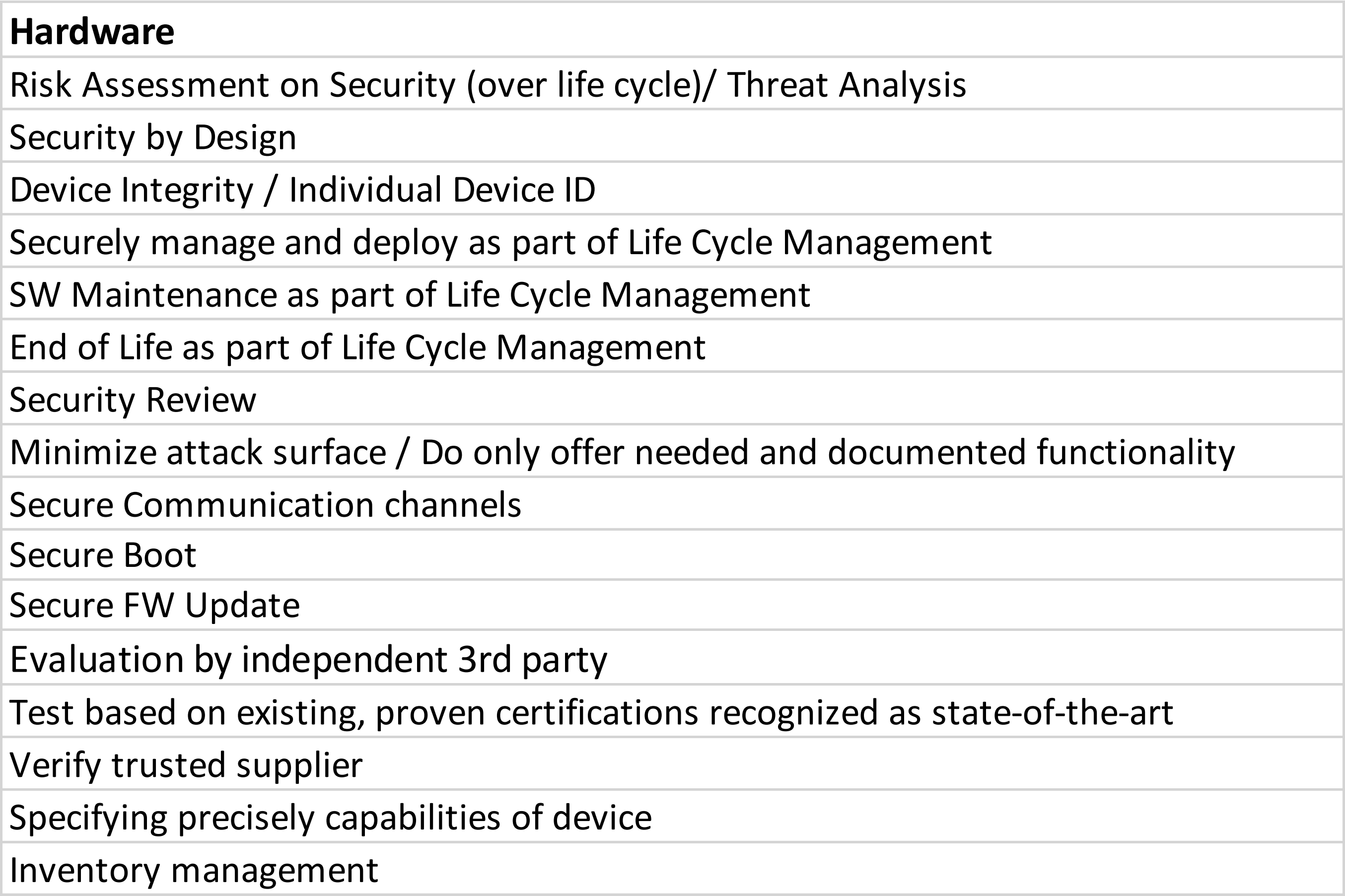
Service
Availability
Safety of disconnected devices
Updatability / Service life-cycle management
Support
Autonomic services provisioning
Incident response model & management
Recovery model
Sunset model

Software/Application



Software/Application
Security Design & Coding Principles
End-to-End Security
Secure Integrity of Applications & Apps
Role based access control for Applications & Apps
Command verification based on context
SW Protection & Maintenance
SW Update / Software life-cycle management
Interoperability of components and communication protocols
Authenticate Identities among themselves
Authenticate messages
Implement consistency checks
Vulnerability Handling
Sharing information about vulnerabilities between stakeholders
Authentication of the App
Authenticity of the App source website
Secure download of Apps/Applications
Secure OS
Reset mechanism
Logging & Monitoring
Firewall / SDP architecture
SW & Apps isolation

Hardware



Hardware
Risk Assessment on Security (over life cycle)/ Threat Analysis
Security by Design
Device Integrity / Individual Device ID
Securely manage and deploy as part of Life Cycle Management
SW Maintenance as part of Life Cycle Management
End of Life as part of Life Cycle Management
Security Review
Minimize attack surface / Do only offer needed and documented functionality
Secure Communication channels
Secure Boot
Secure FW Update
Evaluation by independent 3rd party
Test based on existing, proven certifications recognized as state-of-the-art
Verify trusted supplier
Specifying precisely capabilities of device
Inventory management

Authentication

Authentication
Use of Strong Authentication
Authorized Access to Data
Identification after Authorization
Secure storage of keys
Revocation process
Management of administrator privileges
Authorized to process data, …
Certificate evaluation

Architecture/Network

Architecture/Network
Transparency of Security Architecture
Make us of cryptographic principles and key management
Root Authority
Use state-of-the-art, standard and proven protocols
Network isolation
Proximity detection
Cloud Security
Secure User Access using strong Authentication
Restrictive communication

SECURE CONNECTIONS
FOR A SMARTER WORLD