AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Report

Report on Workshop on Security and Privacy in the Hyper-Connected World

2016

Executive Summary

The Internet of Things ("IoT") – multitudes of smart devices connecting and communicating with each other through one or several heterogeneous networks– is predicted to become ubiquitous within the next five years. However, it is also a development that exposes users to risks. In the IoT, every networked device is a potential target for hackers, and it is likewise a challenge to trace the data flows and functions actually carried out by so many connected devices.

To strengthen the trust of citizens, consumers, businesses and other persons and organisations on the demand side in their networked day-to-day and commercial life, basic requirements for security and privacy are called for that minimize risk, are neutral in technological terms, and remain open to innovation.

Based on the EC Digital Single Market technologies and public services modernisation package published on 19 April 2016, the European Commission is asking about IoT relevant Actions from Standardisation Communication. A workshop was therefore organised by AIOTI on 16 June 2016 in Sophia Antipolis, France, hosted by ETSI to explore the options and guiding principles.

The four breakout sessions at the workshop each focused on a key layer of IoT devices and systems for which design principles are relevant:

- **Session 1: Practical privacy in IoT**
  This breakout session addressed personal data protection issues, drawing initial conclusions on the combination of elements, components and other basics that are deemed to be a minimum prerequisite for a generic baseline for IoT ecosystems. These are: clear taxonomy, mapping & categorisation, clear rules on data ownership and data control (basically, the data subject should stay in control), and rules on which entities are permitted to access and use data and for what purpose. There also needs to be an understanding of the personal data lifecycle (what can happen and happens to data in its life cycle?). The balance between security and personal data protection was discussed, as was the need to support data subjects on make informed decisions about and manage opt-ins, opt-outs and rights management, as well the need to ensure transparency, and appropriate measurements and monitoring when collecting and using personal data.

- **Session 2: IoT hardware and components**
  This breakout session covered the minimum security requirements for the physical layer. In order to minimize the risk of vulnerabilities, IoT devices should only be able to perform functions that are actually documented and make sense for the device. Whichever features and methods are used to uphold security, it is essential that the format be as easily auditable as possible. The security rationale expressed by the designer must be auditable by an independent third party. The framework to deliver the certifications would ensure an "equal level playing field" for all participants, since all actors would adopt the same rules.

- **Session 3: Interfaces and communications**
  This breakout session covered the basic security requirements of the interfaces/protocol stacks. Beginning with discussion on threats to be addressed (e.g. data theft, DoS attacks, risk of device cloning), the group considered the need for managed security – the features of which must also include knowing what action to take in the event security is breached. The ownership of the data generated by an object also has to be clarified. The group was clear that there is no point having a "Trusted IoT Label" that is a marketing label only. It should provide a baseline requirement of protection and a clear visibility of the security achieved. There should also be at least some certification by an independent third party. Close cooperation with the association is necessary in which companies can participate to obtain certification as trusted manufacturers

- **Session 4: Applications**
  This breakout session looked at the minimum security requirements for software applications communicating with other devices in the network and with the cloud. There are two main types: devices with a closed set of apps (routers, thermostats, etc.) and devices that also run third-party apps (e.g. TV set-top boxes). With the second type, manufacturers could (and should) set the rules for third-parties to ensure that the software is compliant with the specified rules. The question of what exactly can be certified was also investigated (e.g. capabilities and performance). The group also examined the challenges in security for applications: if a device has encryption abilities, all the aspects of cryptographic principles and key management are extremely important and should be carefully described in a standard. Also, since most software developers use third-party software, it is important to set rules that define exactly who is responsible for maintaining these libraries and checking for vulnerabilities

The resulting rules – which need to embrace all sectors and all the components, as well as address overall system architecture to ensure data security and privacy in device communication – shall guide common tools, approaches and instruments such as standards, certification, self-regulation, regulation and labelling.

Table of Contents

Executive Summary 2

Background 5

Objective and Outcome of the Workshop 6

Breakout Session 1: Practical Privacy in IoT 7

Breakout Session 2: Components + Devices/nodes + Software (on device) 11

Breakout Session 3: Interfaces, Communication & Cloud 13

Breakout Session 4: Applications 15

Background

The Internet of Things ("IoT") – multitudes of smart devices connecting and communicating with each other through one or several heterogeneous networks– is predicted to become ubiquitous within the next five years. Like any technological advance, IoT offers great opportunities to society and the economy. However, it is also a development that harbours substantial risks:

- In the IoT, every networked device is a potential target for hackers – from the control system of a car's steering to interference with the functioning of an anaesthesia device. In by far the majority of cases, it is the weak points in an IoT ecosystem that hackers target in order to gain unauthorised access.

- In general, no user of a networked device – be it a business or a consumer – can be absolutely sure that the device only features those functions and only executes those data flows that have been specified by the persons or bodies authorised to do so. Thus for devices in the IoT, it is quite a challenge to trace the data flows and functions actually carried out.

To strengthen the trust of citizens, consumers, businesses and other persons and organisations on the demand side in their networked day-to-day and commercial life, basic requirements for security and privacy are called for that minimize risk, are neutral in technological terms, and remain open to innovation.

These requirements need to embrace all sectors and all the components, ranging from simple devices such as smart thermostats to complex IoT systems such as connected cars. They also need to address the overall system architecture in order to enable devices to communicate in a manner that ensures data security and privacy to common standards. The resulting rules shall guide common tools, approaches and instruments such as standards, certification, self-regulation, regulation and labelling.

The layers shall be further elaborated as work continues.

Objective and Outcome of the Workshop

Based on the EC Digital Single Market technologies and public services modernisation package published on 19 April 2016, the European Commission is asking about IoT relevant Actions from Standardisation Communication (point 3: “Explore options and guiding principles, including developing standards, for trust, privacy and end-to-end security, e.g. through a 'trusted IoT label').

To discuss the minimum security and privacy requirements along the entire networked architecture and value chain similar in various sectors, a workshop was staged by AIOTI on 16 June 2016 in Sophia Antipolis, France, hosted by ETSI.

Four breakout sessions were held at the workshop, focusing on the four key layers of IoT devices and systems for which design principles are relevant:

1. Practical privacy in IoT
2. IoT hardware and components
3. Interfaces and communication
4. Applications

This report summarizes the results of the four breakout sessions.

Breakout Session 1: Practical Privacy in IoT Device

In General

The paragraphs below form the combination of elements, components and other basics that are deemed to be prerequisite to address the discussion on minimum requirements for a generic baseline for IoT ecosystems, whether networks, infrastructures, devices, applications, services or data-related. This workshop leverages on the discussions and work done already at the AIOTI WG03 Privacy in IoT taskforce and WG04:

A. Domain

This breakout session addressed the personal data protection of IoT. The domain and dialogue of the workshop zoomed in on the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS) as the main purpose of all workshops was focussing on the generic baseline for all IoT and all IoT ecosystems – whether vertical, horizontal, crossed or otherwise – while identifying minimum requirements for that baseline. It was however understood that other regulations and standards may be relevant as well.

To keep the dialogue focussed, this workgroup also carved-out special or other more extraordinary elements and components, such as highly sensitive personal data, nuclear energy critical infrastructures and the like. With that focus, participants discussed the generic baseline of privacy in IoT.

B. Mapping & Categorising

Next, the group went back to basics, as that is where discussions in most cases already derail as the participants in such discussion do not have or try to find common understanding on the taxonomy. The basic taxonomy does not need to be perfect, but sufficiently workable. Definitions that were established as prerequisite were data, personal data, data controllers and other actors, the personal data life cycle, IoT ecosystems and last but not least the physical and virtual ‘Things’. These have been both segmented, mapped as well as categorised and where relevant classified.

The AIOTI WG03 Privacy in IoT taskforce ‘As-If’ privacy principle, which can be summarised as the principle to design and engineer ecosystems in IoT as if these will (now or in a later phase) process personal data, was also endorsed by the participants. The As-If principle is closely related to the privacy by design and privacy by default principles.

The main stakeholders were – in line with the GDPR – established as (i) data subject, (ii) data controller, (iii) data processor, and (iv) data protection and other authorities, where the data accessor was added to address a mixed group of entities that are able to access data either on an authorised or non-authorised grounds. It was discussed that the actors mentioned above can be a person, organisation, machine or algorithm. Furthermore, the mentioned authorities can be data processors or data controllers themselves as well.

Both taxonomy as well as segmentation, mapping and categorisation are seen as prerequisite elements to define a minimum baseline for privacy in IoT.

C. Data Ownership or Data Control

When asked ‘what do you like about privacy?’ the majority of the participants of the group mentioned ‘control’, in the sense of as a data subject being able to control who can access it and who can use it for what purpose. When we asked ‘what do you miss out in privacy in practice?’ the majority of participants mentioned ‘control’ again. The concept of ‘owning’ your digital personal data was found to address this main privacy principle less well than data control.

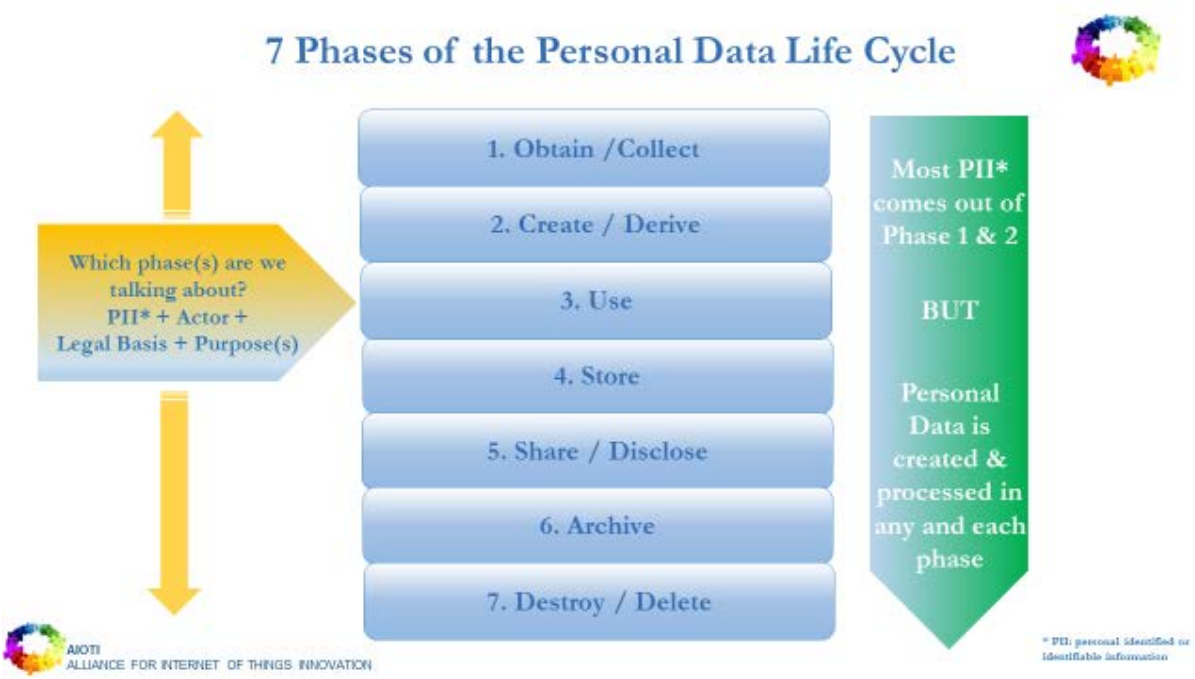
It was understood that basically the data subject should be its own personal data controller. Use in the GDPR of ‘data controller’ is for that matter confusing, and for purposes of the discussion was mentioned as the ‘principle data processor’. This is higher responsibility than subcontractors and other data processor(s) in the data value chain.

D. Access, Use & Purpose

Starting from the basis set forth above, where the data subject is in control of its personal data, the first subsequent minimum baseline topics are access, use and purpose. Data minimisation, accountability, data isolation (unlinkability) and purpose limitation were discussed as baseline essentials for all three topics.

E. Personal Data Life Cycle

To understand and engineer personal data protection, also in order to arrive at a generic baseline for IoT ecosystems, it needs to be clear where and when in its life cyle (as per the ‘As-If’ principle set forth in paragraph B above) a device or other ‘Thing’ as well as the other components of the relevant ecosystem (networks, infrastructures, applications, services or data) comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data. Any personal data in any and each of the personal data life cycle phases means ‘processing’ as defined in the GDPR.



F. Data Security Measures

Obviously – important and a baseline requirement by default – security of personal data was discussed, taking in the elements of data security: availability, integrity, confidentiality, transparency, unlinkability/isolation and intervenability. Data minimisation was again mentioned: the less data an actor can access, the less risk there is of a security breach. Moreover, if data is minimized based on a specific purpose, there is less chance that the actor will breach trust (and the law). The balance between security and personal data protection was discussed as well by means of the questions: how to balance security in privacy?, and how to balance privacy in security?

G. Transparency, Measurement & Monitoring

When personal data is obtained, collected, created or derived on valid legal grounds (for instance as per the prior informed and unambiguous consent of the data subject, per mandatory obligation or other valid legal basis set forth in the GDPR) and accessed, used and otherwise processed for a specific purposed in an adequately secure manner, the important components of a generic baseline are: transparency, accountability, measurement and monitoring:

Transparency: a data subject should be able to know who is taking what action with its personal information.

Accountability: any data processor – not only the data controller as defined in the GDPR – is accountable for regulatory and contractual compliance to the extent concerning its level of processing, the related privacy impact assessment and data subcontractors involved.

Measurement: compliance, being qualitative in nature, is a challenge to measure although it is not impossible. Quality can in many cases be qualified and otherwise measured. However, the challenge is exacerbated when one considers compliance necessary on multi-purpose and data aggregating devices – such as smartphones, or such smart devices communicating

with and through smart vehicles in smart cities.

Monitoring: monitoring includes without limitation logging, reporting and auditing, for which one in some cases may wish to use measurements although it is not necessary in many cases.

In any case, the participants were unanimous that data compliance, transparency and accountability and on the other hand measurement and monitoring thereof, to whatever extent possible, are baseline components to build trust in IoT. Contextuality, also relevant for multipurpose devices, was added to the baseline list as per the nature of IoT and 'Things': even though compliance to access and use certain personal data for one purpose on one device does not lead to automatic compliance for such access and use for other purposes on the same device.

H. Awareness

The last component discussed in this workshop was awareness: the human-focused part of personal data protection. The data subject needs to be aware of privacy issues, choices it makes and possible consequences thereof. However, awareness was also identified as a prerequisite on the vendor / data controller/processor side. Even if data subjects are required to give consent to certain data processing, in many cases they fail to understand what they are actually consenting to because of broad, vague or otherwise unclear wording in privacy policies.

As solution directions, the personal data custodian or thrusted third party was brought up and discussed that helps and supports data subjects with managing personal data, related access and use as well as the monitoring of regulatory and contractual compliance. The other direction was aimed at the vendor / data controller/processor side, the aim being for them to improve and shorten privacy policy and other documentation, while making it easy to read. The wording of sections requesting consent (constituting the practical deployment of related obligations under the GDPR) should be transparent and unambiguous, with easy means for data subjects to change their minds at any time.

I. Other Topics

Security breach and privacy impact assessments were discussed as well. On the vendor side (vendors are required by law to produce a risk impact assessment that also specifies what would happen in the event of a security breach), there needs to be a clear statement on the impact if data is lost. Cloud service providers, for example, could heat-map potential breaches of personal data to show data subjects where they are potentially at risk. Could the market self-regulate or discipline itself? Voluntary mapping of risk would be an option; alternatively, it may be more centralised and certified by an entity such as BSI. In the Netherlands, for instance, internet shops are certified by a voluntary label, and – despite the voluntary nature – the label does serve as a baseline assurance to customers that the provider meets certain standards (like travel agency certification).

The session also looked at examples of best practice from other industries, mainly because IoT represents a convergence of many sectors. By leveraging expertise from other industries, it would be possible to adopt practices with proven value for IoT.

Other relevant topics were touched on but as per time limitations not yet discussed in detail – such as consequences and possible baseline components related to
(i) personal data breach notifications – how (customer, data subject & data protection authority) and within what timeframe
(ii) data portability, migration, and transfer back assistance (formats, costs), data retention, restitution and deletion (duration, return process, level of deletion) and cooperation (actors interacting with data subject on data access, correction rights and the right to be forgotten, as well as legally required disclosures to law enforcement authorities.

However, participants confirmed they would continue the dialogue through the channels of AIOTI WG03 Privacy in IoT taskforce and WG04, after which this workshop meeting was adjourned.

Basic Requirements on PRACTICAL PRIVACY IN IoT:

- **Common Understanding**
  Design, manufactor and assemble components of Things and IoT ecosystems with clear understanding of what means what, and to what extent there is consensus in the related complex value chain and ecosystems. Promoting the goals of data protection such as limiting the scope of data processing to the necessary level; data segmentation, mapping, categorisation, purpose limitation, data isolation, and data control and data access of personal data are seen as prerequisite elements.
- **No Personal Data by Default, 'As-If' by Design & De-Identification by Default**
  Data minimalisation starts with only requesting, collecting, obtaining, deriving and processing personal data to the extent necessary (need-to-know principle), and. The 'As-If' principle it to design and engineer ecosystems in IoT as if these will (now or in a later phase) process personal data. The As-If principle is closely related to the privacy by design and privacy by default principles. Design de-Identification capabilities so personal data is de-identified as soon as legally possible.
- **Manufacturer-Implemented Parametrization**
  Rights management for accessing data controlled by the user based on the assessment where and when a Thing or IoT ecosystems in its lifecycle comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data, while keeping in my mind the contextuality of purposes and use, as well as multi-purpose Things and IoT ecosystems.
- **Accountability & Risk Impact Assessment by Design**
  Any data controller and processor to be accountable for regulatory, contractual and ethical compliance. If data is compromised, disclosed, accessed or lost, clear statement by vendors, data controllers and data processors on impact is another prerequisite.
- **Awareness & Information Supplied with Indication of Purpose**
  Technically regulating access to data to define who can use it for what purpose, and how that can be made transparent, and subsequently measured and monitored. Design in a transparent way, so the data subject is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.

Breakout Session 2: IoT Hardware and OS: Components + Devices/nodes + Software (on device)

This breakout session covered the minimum security requirements for the physical layer such as semiconductor components, application microcontrollers, secure elements and sensor ICs, devices/nodes such as gateways, bridges, actuators and sensors, as well as on-device software.

Results

The session began with a discussion of the risks: an IoT device is usually not operated in a safe environment, and it is possible for hackers to obtain such devices and attempt to locate the key material on the device microchip. It is therefore necessary to make the chips secure enough to prevent data and key material from being manipulated by third parties.

In order to assess the security risk, one must first carry out a security analysis, e.g., identify the threats, the assets to be protected and the level of desired security also has to be decided. The challenge is that the developer/actuator might not know in which system or environment the device will later be used. This can be countered effectively by introducing a classification (or certification) system that would certify devices for use in particular use case scenarios depending on the level of risk. With this type of system, it would be possible to prevent devices entering the market without the appropriate security.

Analysing the security requires getting from the designer of the IoT device a clearly expressed security rationale that explains why he believes the security measures that have been implemented are an answer to the security risks. The security rationale needs to be auditable by an independent third party. If a microchip is unprotected, for example, it will be assigned level 0. Certified tamper-resistant ICs offer secure storage for key material and certificates and also various certified crypto functionalities. Standardization on interoperability of components and communication protocols will also be required.

It is clear that security of devices depends heavily on the security of their components, and also how these components interact. both for the hardware and the software components. As an example for the hardware, appropriate protection should be put in place to prevent communications on the PCB from being intercepted – which would give hackers access to data.

Sharing knowledge is also important: manufacturers could be encouraged (or required) to share information about security incidents in order to warn other manufacturers of potential vulnerabilities and enable them to take prompt action (the down side here is of course that such information would also be of interest to potential hackers).

In order to minimize the risk of such vulnerabilities, IoT devices should only be able to perform functions that are actually documented and make sense for the device. Likewise, credentials should not be hard-coded into a device. The elimination of hard-coded credentials ensures that the keys are not easily interchangeable between devices, preventing hackers from targeting weak points. This is of prime importance, also in preventing data transport from being intercepted. Secure E2E transport is also essential, but the transport path also becomes open if a hacker manages to access the device credentials.

Raising security also involves having a safe place to store data at rest – for credentials and also for the secure boot process. The secure boot accesses key material and only starts the device if the key is correct. The IoT device must also be able to detect any anomalies, i.e. be able to tell if it is under attack. Features similar to those used with bank cards could be applied – the device could be rendered tamper-resistant by only permitting a certain number of access attempts before it auto-deletes its key material.

Formats and frameworks
Whichever features and methods are used to uphold security, it is essential that the format be as easily auditable as possible. Evaluation can soon become complex, so a use case-based approach might also be feasible (with security profiles for specific applications).

The actual “security label” should also be considerably more than a sticker! If details are also made electronically accessible, and connected to a security certificate, other devices will be able to check and verify the certificate regularly, and halt communication if there is any sign of compromise. If an IoT device is potentially compromised, the label must be dynamic enough to indicate either danger or a warning, and the certification can be restricted or cancelled the moment a microchip is compromised by attack. Related information can be requested by the user e.g. via Smartphone using NFC or BLE for connectivity to the IoT device.

The framework to deliver the certifications would ensure an “equal level playing field” for all participants, since all actors would adopt the same rules. The technical guidelines or certification for IoT devices should preferably be based on simple mechanisms that take into account the non-critical nature of many of these devices. This comes with a caveat: smartphones, for example, which are connected to those IoT devices, can track a substantial amount of personal data through their apps, and any certification levels should also take these privacy issues into account. Technical Guidelines based on internationally accepted rules like CCRA and SOGIS-MRA should be initiated and led by e.g. ANSSI and BSI. Gaps should be analysed by ENISA and standards further developed by ETSI.

The breakout group did not reach consensus on whether such guidelines should be mandatory – this is therefore a question requiring further investigation.

Key directions
A key next step in this process will be to release and distribute an action plan with clear timing on milestones, also including details on what exactly needs to be done in order to do justice to the baseline requirements that have been set out.

Basic Requirements on IoT HARDWARE AND COMPONENTS:

- **Testing and Certifying Security**
  Using existing, proven certifications recognized as state-of-the-art based on assessed risk level; additional introduction of a classification system to certify devices for use in particular use case scenarios depending on the level of risk.
- **Security Labels**
  Proven labels like the 'Energy efficiency label' of appliances will classify the IoT device.
- **Preset Certified Security Structures**
  Encryption requirement for identities, access, communication channels and secure storage of keys and to store data at rest – also for secure boot process.
- **Security Rationale**
  Required explanation of implemented security measures related to expected security risks from any designer of IoT device, auditable by independent third party.
- **Information exchange**
  Sharing information about incidents/potential vulnerabilities between manufacturers.
- **Defined functions**
  IoT devices should only be able to perform documented functions, making sense for device/ service.
- **Standardisation**
  Interoperability of components and communication protocols.

Breakout Session 3: Interfaces, Communication & Cloud

This breakout session covered the basic security requirements of the interfaces/protocol stacks (such as CAN/AutoSAR, OPC-UA, 801.11x, ZigBee, EEBUS, OSGI, Threat, AllJoyn, etc.) used in various sectors as well as the network, e.g. in the Wide Area Network, towards the backend system and also for cloud-based applications. Very often security is not covered by communication stacks today, and there are no minimum encryption requirements.

Results

The session began with a general discussion of the threats to be addressed:

- Possibility that devices could be controlled or taken over by unauthorized third parties
- Data theft
- DoS attacks
- The risk of breaches of confidentiality of communication
- Risks that device identity could be compromised
- Risk of device cloning

It is necessary to consider many co-existing types of gateway: for example, even if all are connected to the cloud, some are connected to local networks behind the gateway. It is important also to consider the IoT-based devices that are exposed to the cloud because they are connected to a router.

Smart devices may be connected and communicating through heterogeneous networks, with specific constraints. In some applications, speed plays a key role, as does the need for low latency, and security measures also have to take this into account. Security must be able to work for both very high and very low bandwidth, and if security cannot be accomplished at the connectivity level, it has to be devolved to application level.

Managed security is a requirement – and this also includes knowing what action to take in the event security is breached. Likewise, concerning data privacy, the relationship between people needs to be reflected in terms of interoperability. The ownership of the data generated by an object also has to be clarified.

Trusted IoT label:
There is no point in having a marketing label only. The label should give a baseline requirement of protection, and the level of assurances for this need to be defined. The label should provide a clear visibility of the security achieved.

Possible levels of security:

4) Security Certified by third party
3) Managed Security (maintained)
2) Secure Update mechanism implemented (maintainable)
1) Access Controlled device, based on “trusted manufacturer” and self-assessment of security
0) No security

The security baseline provides a very basic minimum level, and there should be multiple trusted IoT levels, each with successively strict levels of security.

Minimum requirements:

A security checklist is not enough to provide the necessary level of trust, and something more than self-security assessments will be needed – at least some certification by an independent third party. There is the risk that an untrusted IoT device will be connected to a secure system or network. Therefore, the manufacturer need to be trusted. A signature process is requested to check if such manufacturer can be trusted before any authentication process will take place and the IoT device will be connected to a secure network. Close cooperation with the association is necessary in which companies can participate to obtain certification as trusted manufacturers.

Layering and partitionning security features, with associated baseline requirements could help to manage scalability, evolutivity and risk assessment of the overall IoT system:

- Identification and authentication of end-devices, gateways and servers as very first requirement.
- Connectivity security requirements
- Applicative security requirements

Authentication at device level is needed, but this raises the question of where to store certifications; it makes sense to segment authentications into “levels” – higher-level devices need to be able to detect other devices with lower security levels than their own.

Other features that managed security must have:

- Revocation functionality
- Must be easy to adopt and to design in
- Must have multiple security levels
- Functionality reduced to purpose of use case
- Remote attestation
- Integrity of SW & HW: Code signing (HW/SW/etc.)

Basic Requirements on INTERFACES, COMMUNICATION, CLOUD:

- **Security and data**
  Management process and clarification of ownership required; easy to adopt; data should also be encrypted on the application layer; all aspects of cryptographic principles and key management are extremely important and should be carefully described.
- **Authentication of Identities Among Themselves**
  Open to all technologies and applications.
- **Specification of Security Levels**
  Security level 0-4 fit to the market understanding; a related Trusted IoT Label should give a baseline requirement of protection based on the level of assurances and robustness.
- **Certification procedure**
  Specifying precisely capabilities of device of a particular type; partitioning security evaluation & certification based on defined features of Managed Security could help to manage liability and evolutivity on system level.
- **Standardization**
  All aspects of cryptographic principles and key management to be carefully described.

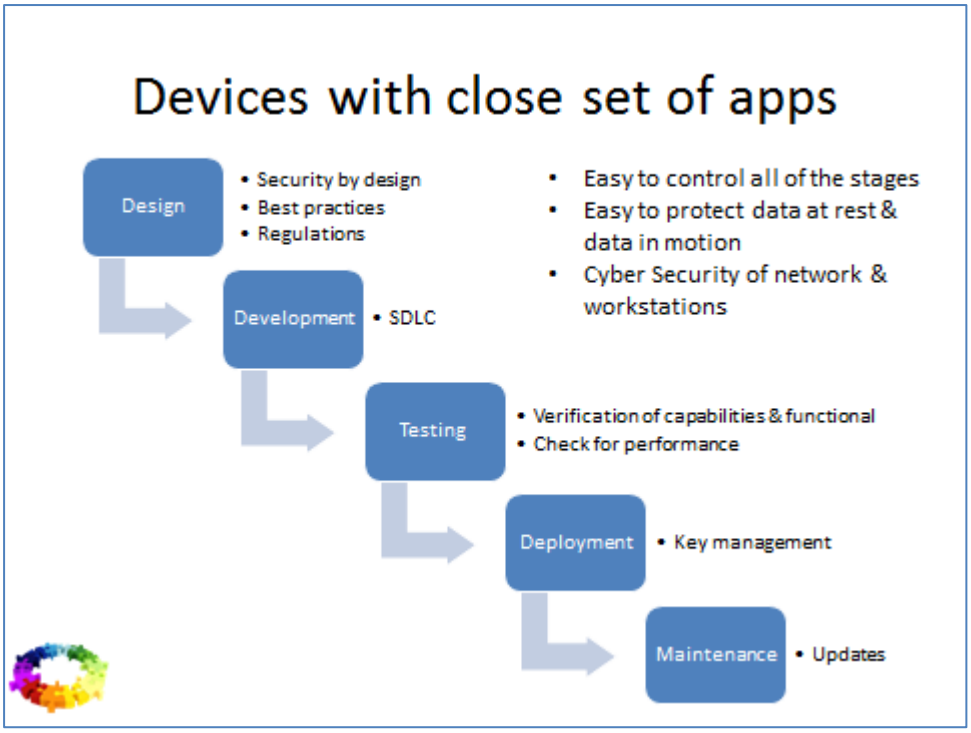
Breakout Session 4: Applications

This breakout session looked at the minimum security requirements for software applications communicating with other devices in the network and with the cloud.

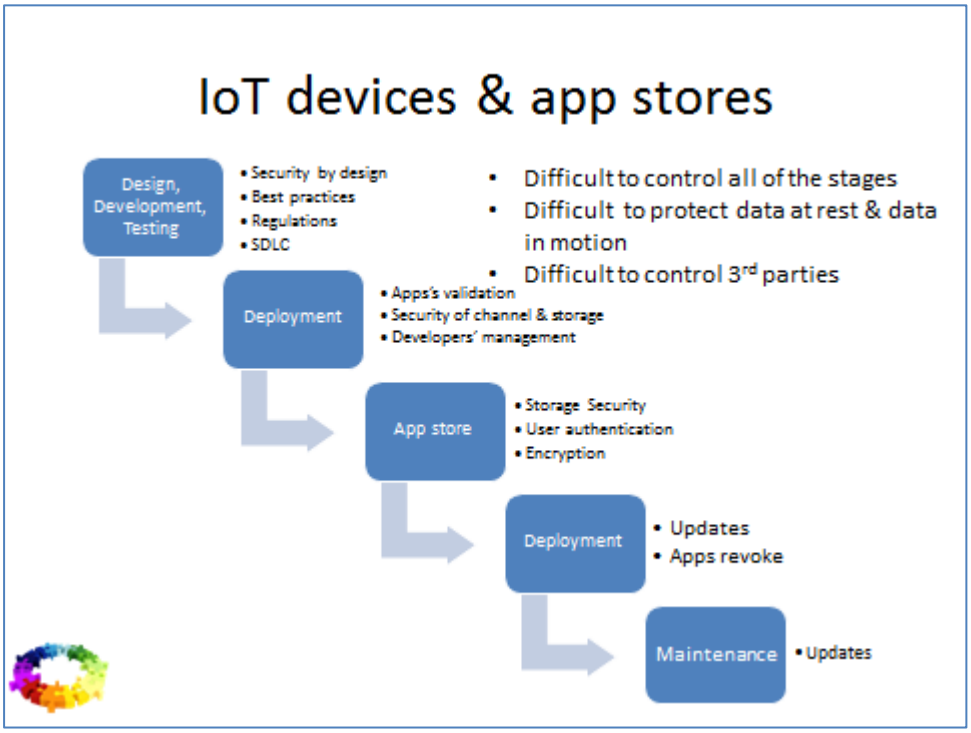
Results
The role of the label or specification is to assure the customer that a device carrying the logo is safe and secure, and will remain so in the future.
It means that software developer has to keep a software in an actual state thru a software's entire lifecycle.

There are currently two main types of software that are by nature used in embedded devices:

- Devices with a closed set of apps (routers, thermostats, etc.)



- Devices that also run third-party apps (e.g. TV set-top boxes, car IVI, smart home hubs, etc.)



With the first type of device – more common in the market – manufacturers have total control of the entire manufacturing and software development lifecycle, from design to maintenance. This makes it easy to protect data and control the quality of software and hardware.

The situation is different for devices that are able to download and execute third-party software. Here, manufacturers could (and should) set the rules for third-parties to ensure that the software is compliant with the specified rules.

Certification
The question of what exactly can be certified was also investigated.

- Capabilities – the features or abilities that a piece of software should have, such as the ability to secure incoming and/or outgoing connections, update firmware securely, log events and detect anomalies. Any certification procedure should specify precisely what capabilities a device of a particular type should have
- Performance – are all the capabilities implemented in the code?

This is similar to the V-cycle, where we first design and declare what we need to implement, and then verify if all of the features were implemented correctly.

Challenges

There are two key challenges in security for applications:

End-to-end security and key management

Data should be encrypted on the application layer. If a device has encryption abilities, all the aspects of cryptographic principles and key management are extremely important and should be carefully described in a standard.

Third-party libraries

Most software developers use third-party software (for example Open SSL library). It is important to set rules that define exactly who is responsible for maintaining these libraries and completing work such as updates and checking for vulnerabilities.

Basic Requirements on APPLICATIONS:

- **Encryption**
  Data should be encrypted on the application layer. End-to-End Security , cryptographic principles and key management are extremely important and should be carefully described.
- **Accountability & Liability**
  Manufacturers must be accountable and liable as they have or should have total control of the entire design, manufacturing and software development lifecycle; to execute third-party software the manufacturer should set the rules to ensure that the software is compliant with them.
- **Third-party libraries**
  Rules for maintaining, updates, checking for vulnerabilities.