



Security and Resilience of Smart Home Environments

Good practices and recommendations

DECEMBER 2015



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Cédric LÉVY-BENCHETON (ENISA), Ms. Eleni DARRA (ENISA), Mr. Guillaume TÉTU (Trusted labs), Dr. Guillaume DUFAY (Trusted Labs), Dr. Mouhannad ALATTAR (Trusted Labs)

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

Dr. Serge AUTEXIER (German Research Centre for Artificial Intelligence – DFKI)
Eng. Thierry BOUSQUET (ST MICROELECTRONICS)
Dr. Andrei COSTIN (Firmware.RE)
Mr. Thomas GAYET (CERT-UBIK)
Mr. Filip GLUSZAK (GridPocket)
Ms. Svetlana GRANT (GSM-A)
Mr. Abraham JOSEPH (IOT Insights)
Dr. Thibaut KLEINER (European Commission)
Dr. Gert LÆSSØE MIKKELSEN (Alexandra Institute)
Mr. Brian KNOPF (BRK Security / I am the Cavalry)
Mr. Kai KREUZER (openHAB)
Mr. Antoine LARPIN (Panasonic)
Mr. Jan-Bernhard de MEER (smartspace laboratories GmbH)
Mr. Cédric MESSEGUER (Digital Security)
Mr. Chris de MOL (Fifthplay)
Mr. Christian MÜLLER (University of Mannheim)
Mr. Detlef OLSCHESKI (Cleopa GmbH)
Ms. Barbara PAREGLIO (GSM-A)
Mr. Antonio PELLICCIA (IBM)
Mr. Gaus RAJNOVIC (Panasonic)
Mr. Hartmut RICHTHAMMER (University of Regensburg)
Mr. Mathieu SACRISPEYRE (INTESENS)
Mr. Benjamin SCHWARZ (CTOi Consulting)
Mr. Ian SMITH (GSM-A)
Mr. Craig SPIEZLE (Online Trust Alliance)
Dr. Pavel TUČEK (Cleopa GmbH)

Dr. Steffen WENDZEL (Fraunhofer FKIE)
Mr. Peter WOOD (First Base Technologies)
Mr. Andrej ZIEGER (DFN CERT Service GmbH)

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2015
Reproduction is authorised provided the source is acknowledged.

ISBN: 978-92-9204-141-0 | doi:10.2824/360120

Table of Contents

Executive Summary	6
1. Introduction	8
1.1 EU Policy	8
1.2 Scope of the study	9
1.3 Target audience	10
1.4 Methodology	10
1.5 Outline	10
2. The Smart Home Environments	12
2.1 Overview	12
2.1.1 Connectivity	12
2.1.2 Classes of IoT devices	13
2.2 Threats to Smart Home Environments	15
3. Key Findings	16
3.1 The need for security in Smart Home Environments is still underestimated	16
3.2 Vendors lack incentives to enhance security in Smart Home devices and services	17
3.3 Smart Home devices and services implement few security measures	17
3.4 Smart Home Environments result in new security challenges	18
3.5 IoT vulnerable “building blocks” cause vulnerabilities to be shared at large scale	19
3.6 IoT pervasiveness and dynamicity	19
3.7 IoT brings new constraints on security	20
4. Good practices for a Secure Smart Home Environment	21
5. Good practices for the development of Smart Home devices and services	22
5.1 Security of the development process	22
5.1.1 Design phase	22
5.1.2 Development phase	23
5.1.3 Testing phase	25
5.2 Security functions for hardware and software	27
5.2.1 Security audit	27
5.2.2 Communication protection	28
5.2.3 Cryptography	30
5.2.4 User data protection	33
5.2.5 Identification, authentication, authorisation	35
5.2.6 Self-protection	38
6. Good practices for the integration of devices in the Home Area Network	43
6.1 Minimum reliability	43
6.2 Trust relationships	44
6.3 Network security	46

7.	Good practices for the usage until end-of-life	48
7.1	Protection of data exchanges	48
7.2	Operational security and maintenance	49
7.2.1	Vulnerability survey	49
7.2.2	Security updates	50
7.2.3	Remote interfaces protection	51
7.2.4	Security management system for support infrastructures	51
7.3	Control of user data	52
8.	Recommendations	53
8.1	All stakeholders should reach a consensus on minimum security requirements	53
8.2	Industry actors should support security-driven business models	53
8.3	All actors should contribute to raise security awareness	54
8.4	Industry actors should develop security assessment methods or frameworks	54
8.5	Policy Makers should clarify the legal aspects of Smart Home Environments	55
8.6	Industry research and publicly-funded initiatives should integrate cyber security in R&D projects related to Smart Home and IoT	56
Annexes		
Annex A:	Additional details on Smart Home Environments	57
Annex B:	Mapping threats with good practices	60
Annex C:	Checklist of good practices	68
Annex D:	Example of topics for user awareness	73
Annex E:	List of Acronyms	74

Executive Summary

The Internet of Things (IoT) is an emerging concept where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. In the context of “Smart Home Environments” both IoT and traditional devices and services integrate in a home to enhance the quality of life of citizens. This allows improvements in several domains such as energy efficiency, health monitoring...

New Smart Home devices and services appear at a fast pace, from various manufacturers which may have a limited experience of cyber security. Yet, it is often necessary to integrate these devices in the “Home Area Network” in order to provide connectivity for data exchange and to perform their operations.

Due to these interdependencies, numerous cyber threats appear with possible consequences on the life, health and safety of the inhabitants. Hence, it becomes important for manufacturers, solution vendors, developers, and end-users to understand how to secure devices and services.

In Smart Home environments, the security can be difficult to implement within a heterogeneous ecosystem which integrates several types of devices and services, which usually have limited security due to their weak capacities (CPU, battery...). Moreover the service they provide usually relies on remote infrastructures for cloud storage, analytics or even remote access to the devices.

It becomes necessary to follow a holistic approach of security as the multiple dependencies open new ways of remote attacks, as presented in presented in “*ENISA Threat Landscape and Good Practice Guide for Smart Home and Converged Media.*”¹

The key findings of this study confirm the difficulty to ensure the security of Smart Home Environments:

- The need for security in Smart Home Environments is still underestimated and vendors lack incentives toward this goal.
- It is difficult to understand which security measures can protect Smart Home devices and services, as they present new security challenges due to their interconnected and pervasive nature.
- Many IoT applications, Smart Home devices and services rely on other “building blocks”, which may cause unknown vulnerabilities to appear.

This study aims at securing Smart Home Environments from cyber threats by highlighting good practices that apply to every step of a product lifecycle: its development, its integration in Smart Home Environments, and its usage and maintenance until end-of-life. The study also highlights the applicability of the security measures to different types of devices.

The good practices apply to manufacturers, vendors, solution providers for hardware and software, and developers. It can be used to assess their current security level, and evaluate the implementation of new security measures. European citizens, standardisation bodies, researchers and policy makers could also find an interest in this study.

¹ <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-for-smart-home-and-media-convergence>

The application of good practices aims at covering existing threats. However, Smart Home Environments remains only one specific application of the Internet of Things. Thus, it requires a continuous effort to ensure the security of new devices and services and the safety of its inhabitants.

ENISA proposes the following six recommendations with the objective of enhancing the current status of cyber security in Smart Home Environments and in a more general IoT context:

- 1. All stakeholders should reach a consensus on minimum security requirements:** the development of minimum security requirements should help non-experts in implementing specific security functions in their devices and services
- 2. Industry actors should support security-driven business models:** as Smart Home manufacturers tend to focus on functionalities, security can become a differentiation factor and provide added-value to customers.
- 3. All actors should contribute to raise security awareness:** to help manufacturers with less experience on security and customers, awareness is needed to understand which actions are needed to secure a Smart Home.
- 4. Industry actors should develop security assessment methods or frameworks:** as IoT for Smart Home Environments brings a new paradigm. Specific methods or framework shall ease security assessment and accompany deployment of security measures.
- 5. Policy Makers should clarify the legal aspects of Smart Home Environments:** since there is currently a limited scope in the liability when a device is compromised. With health and safety concerns, policy should help understand the responsibilities and have a preventive role.
- 6. Industry actors and publicly-funded initiatives should integrate cyber security in R&D projects related to Smart Home and IoT:** there are numerous Research and Development projects in the domain of Smart Home Environments and IoT, which could gain impact by integrating specific security aspects.

1. Introduction

Smart Home Environments integrate multiple IoT devices and services that collect, process and exchange data. They provide users several possibilities to control and adapt the status of their home, either manually or automatically. For that purpose, Smart Home devices and services exchange data with internal and external actors. These interactions take place with mobile applications on an end-user's equipment (smartphone, tablet...) and also with remote services in the Cloud.

Due to their interconnected nature, Smart Home devices are subject to a number of security threats either from remote attackers or from inside the Home Area Network (HAN). Moreover, these threats have an impact not only on a user's data but also on his/her health and safety: this changes the accepted idea that the home is usually a safe place to live in.

Smart Home Environments being an emerging domain and because the liabilities are not well defined, it becomes important for all actors to develop adapted security measures to prevent cyber threats. For that purpose, there is a need to secure Smart Home Environments and effectively reduce the threats.

1.1 EU Policy

At the time of this writing no dedicated EU Policy has been identified to target Smart Home Environments specifically.

However, the following general policies on IoT can be extended to this area:

- The Digital Single Market² identifies internet and digital technologies as one of the 10 priorities of the European Commission to foster EU economy with IoT being a key enabler.
- The Opinion 8/2014 on the Recent Developments on the Internet of Things³ identifies *home automation* as one of the three main IoT topics to be addressed in the coming years.
- The EU Data Protection Directive 95/46/EC⁴ with the additional elements from Opinion 03/2014 on Personal Data Breach Notification⁵ covers security of personal data.
- EU Research initiatives such as FIware⁶ and the AIOTI alliance⁷ bring building blocks toward an integrated IoT environment.

Note that no dedicated EU policy covers IoT security either. Indeed, for the European Commission "There is no consensus on the need for and the scope of public intervention in the field of IoT."⁸ Should there be any future development on the EU regulation, it is important to consider the status of cyber security.

² <http://ec.europa.eu/priorities/digital-single-market/>

³ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

⁵ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

⁶ <https://www.fiware.org>

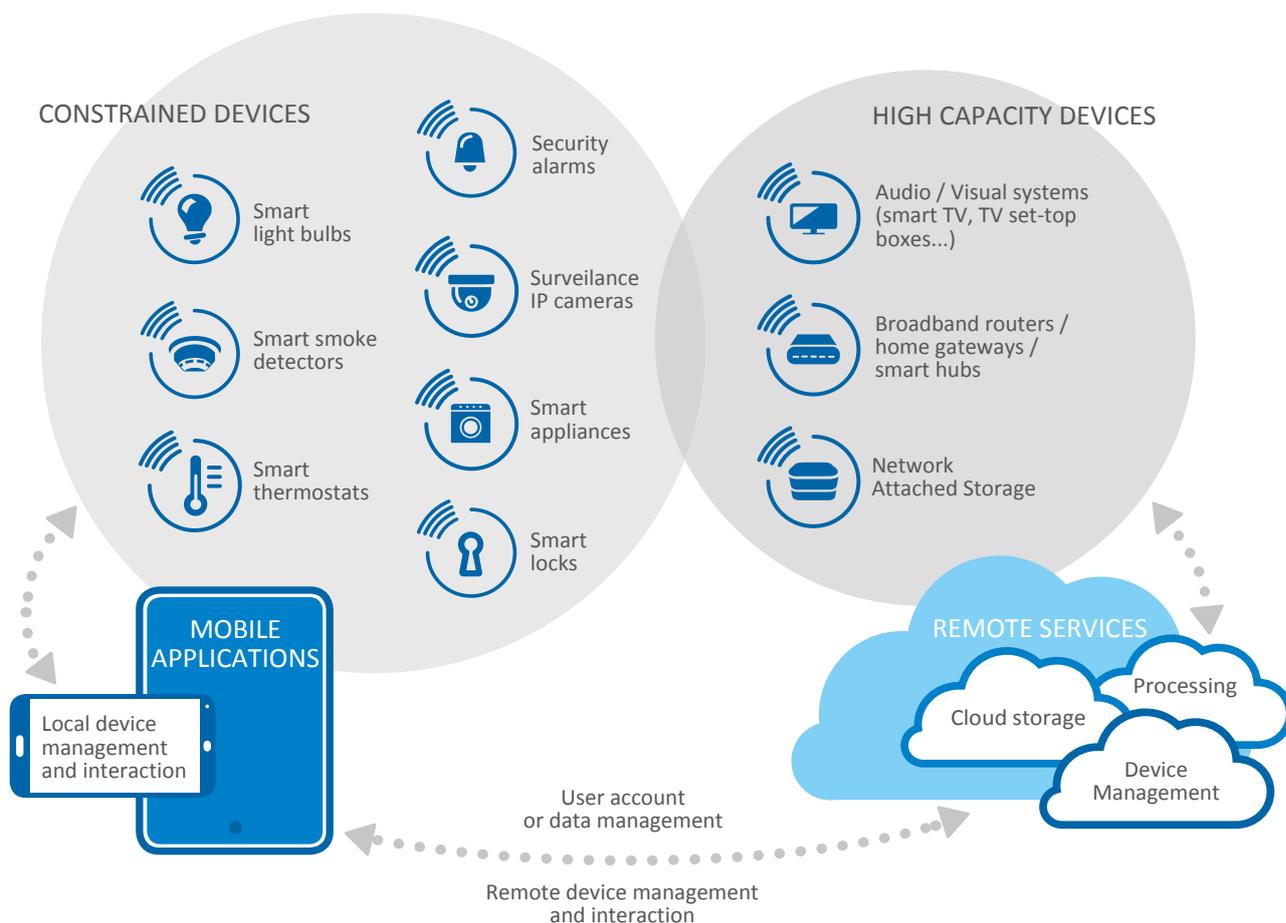
⁷ <http://www.aioti.eu>

⁸ <http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation>

1.2 Scope of the study

This study evaluates good practices to secure the lifecycle of Internet of Things (IoT) products and services in the context of Smart Home Environments.

Figure 1: Scope of the study



As illustrated in Figure 1, this study focuses on:

- **The two types of IoT Devices** that can be found in a Smart Home Environment:
 - **Constrained devices** as defined by RFC 7228.⁹ The security in these devices may be limited due to their comparatively low capacities (CPU, memory, battery...).
 - **High-capacity devices** typically powered by the mains supply. These devices may be able to implement strong to very strong security features as they possess hardware configurations (CPU, memory) that grants them significant computing power.
- **The interactions and data exchange with remote services** including remote activation, remote storage or content, device administration and analytics.
- **The interactions and data exchange with mobile applications** for control/command purposes and data exchange among devices.

⁹ RFC 7228, IETF <https://tools.ietf.org/html/rfc7228>

1.3 Target audience

This study aims at providing simple and pragmatic guidance for securing Smart Home Environments. The main stakeholders that this study targets to include:

- **Smart Home manufacturers and third-party developers** (including HW and SW components vendors, API developers...) as they are the main actors in IoT devices and services for Smart Home Environments.
- **Service and solution providers** (Cloud service providers, Third-party services associated with Smart Home devices...) as they communicate and exchange data with Smart Home Environments.
- **Electronic communications providers** (ISPs, MNOs, MVNOs) due to their implication in bringing connectivity to Smart Home devices and services.

The findings could also potentially interest:

- **Cybersecurity agencies** and/or **Standardisation bodies** for security awareness, device security certification and also security standardisation initiatives.
- **Consumer associations** for end-users security awareness and benchmarking purposes.
- **Policy makers** and **academics** to assess to which extent security can be integrated in their work (new policies, researches, funding...).
- **Hobbyists, enthusiasts and open source contributors** that develop their own Smart Home by writing software or integrating open source software, and use frameworks such as Raspberry or Arduino platforms.

These stakeholders can selectively apply good practices related to the development and usage of Smart Home devices and services, for example in association to a risk assessment. For example, electronic communication providers can implement good practices from the point of view of the local network protection offered by their set-top boxes.

1.4 Methodology

This study is based on a collection of publically available information relevant to Smart Homes which were analysed and correlated to:

- Update the threats applicable to Smart Home Environments.
- Perform an inventory of the good practices identified by the security community in a Smart Home context, or in the IoT context when relevant.

The results were then crosschecked with stakeholders through an online questionnaire and selected interviews with device manufacturers, security experts, standard groups and network operators. This step addressed open questions on emergent and unexpected topics.

The results have been validated by experts in IoT and Smart Home Environments through document review and in a validation workshop.

1.5 Outline

This study is organised as follows:

- **Section 2 “The Smart Home Environments”** defines the type of devices, services and technologies encompassed in this study by the term “Smart Home” and also summarizes threats applicable to these environments.

- **Section 3 “Key Findings”** presents the outcome of stocktaking and interviews with stakeholders from the Smart Home ecosystem with regards to current implementation of security in Smart Home products and Smart Home particularities.
- **Section 4 “Good practices for a Secure Smart Home Environment”** introduces the core of this study. It defines the comprehensive set of security “good practices” applicable to the Smart Home context for mitigating existing threats. These good practices are organized according to the lifecycle of Smart Home devices and services in the following sections.
- **Section 5 “Good practices for the development of Smart Home devices and services”** highlights the good practices to secure the development of Smart Home devices and services.
- **Section 6 “Good practices for the integration of devices in the Home Area Network”** presents the good practices to integrate devices securely in a Smart Home Environments
- **Section 7 “Good practices for the usage until end-of-life”** focuses on the good practices to ensure security for the operation and maintenance of products deployed in Smart Home Environments.
- **Section 8 “Recommendations”** builds upon the gap analysis in order to propose recommendations aimed at improving the level of security in future Smart Home Environments. These recommendations are intended for vendors and service providers, national cybersecurity agencies, consumer groups, standard groups and/or industry associations.

2. The Smart Home Environments

2.1 Overview

The definition of Smart Home Environments is taken from the one found in “ENISA Smart Home threat landscape.”¹ This definition refers to devices and systems present in the Smart Home, the associated services and the networks used to interconnect these devices and services, located inside or outside the home.

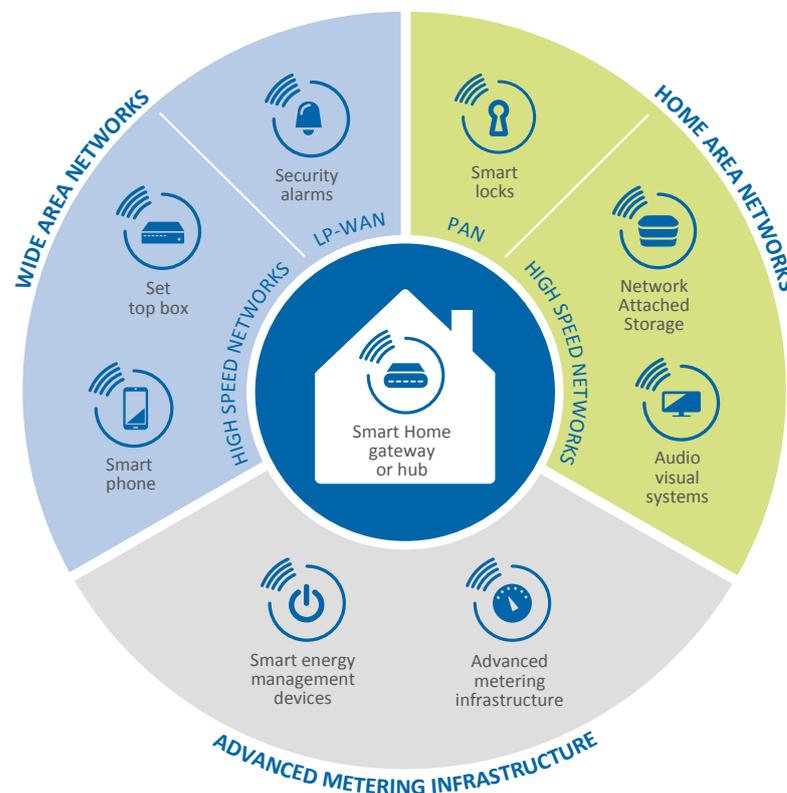
This study is a follow-up of the ENISA Smart Home threat landscape, which presented the various threats applicable to Smart Home. Findings showed that threats target a wide range of applications in the Smart Home and can have consequences on the end-user. For that purpose, it is important to define appropriate security measures that rely on the specificities of the Smart Home.

2.1.1 Connectivity

The common point between Smart Home devices resides in the combination of “smartness” (data processing and connectivity) and the “local” nature of the use case (devices are in the user home). This means in practice that connectivity:

- is always present in the devices, either limited to the Home Area Network or with access to the Internet;
- may be related to several kinds of communication protocols (direct, short-range or long-range, wired or wireless); and
- may lead to several interconnected networks in the home and outside the home.

Figure 2: Example of several network types found in a Smart Home Environment



Such networks are described further in Figure 2. They typically include:

- One or several **Home Area Networks (HAN)**, which are dedicated to local networks or subnetworks for Smart Home devices and sensors:
 - One or several High Speed Networks, usually Wi-Fi networks, that may be provided by a set-top-box, mobile devices...
 - Personal Area Networks or ad-hoc networks created between several devices, for instance using low-speed connections (*e.g.* Bluetooth, Zigbee...).
- Connections to **Wide Area Networks (WAN)**:
 - **High Speed Networks**, typically providing access to the Internet, for instance through the Internet Service Provider (ISP) network or the Mobile Network Operator (MNO) network.
 - One or several **Low Power Wide Area Networks (LPWAN)**, which provide WAN connectivity while requiring low power from the device (*e.g.* LoRaWAN, Sigfox...).
- If the home uses a smart meter, this meter connects the home to the associated **Advanced Metering Infrastructure (AMI)** used to communicate with smart energy management devices.

It should be noted that *real-life* deployments of Smart Home might include only some of these networks, or might use them differently: for example, home automation devices may directly use the home Wi-Fi to access remote services, without using a dedicated gateway.

Note that many elements of the Smart Home have connections to other domains: energy might have connections to the *smart metering* domain, devices related to assisted-living might have connections to the *eHealth* domain, many other devices in the Smart Home might have connections to the *connected mobility or wearables* domain.

These connections might bring additional security constraints to these devices, notably in terms of compliance to national health or energy (critical infrastructure) requirements. This is out of the scope of this study.

2.1.2 Classes of IoT devices

The types of devices taken into account for this study are constrained (defined as per RFC 7228)⁹ and high-capacity ones. Constrained devices are divided into three classes depending on their RAM capacity, memory storage capacity and CPU power. Indeed, the class of a constrained device has an impact on its security capabilities, and thus it introduces limits to the application of some good practices.

Table 1 summarizes the classes of IoT devices based on their hardware properties. It describes the impacts on their security capabilities.

Table 1: Classes of IoT devices and the impact on their security capabilities.

DEVICE TYPE	CLASS	EXAMPLE OF RAM CAPACITY	EXAMPLE OF MEMORY STORAGE CAPACITY	EXAMPLES OF DEVICES	TYPICAL IMPACT ON SECURITY CAPABILITIES
Constrained device	 Class 0	<< 10 KiB	<< 100 KiB	Low-end sensors	Class 0 devices may not be able to implement real security measures

DEVICE TYPE	CLASS	EXAMPLE OF RAM CAPACITY	EXAMPLE OF MEMORY STORAGE CAPACITY	EXAMPLES OF DEVICES	TYPICAL IMPACT ON SECURITY CAPABILITIES
	 Class 1	~ 10 KiB	~ 100 KiB	Smart bulbs, ¹⁰ Smart locks ¹¹	Class 1 devices may use dedicated protocols designed for constrained nodes (such as CoAP) but they cannot use stronger standard security protocols
	 Class 2	~ 50 KiB	~ 250 KiB	Smart appliances, high-end smart sensors (such as smart thermostats)	Class 2 devices have the capacity to implement the most standard security protocols (even if other limitations can cause issues, such as communication bandwidth)
	 High-capacity device	>> 50 KiB	>> 250 KiB	Smart hubs or gateways, Smart TVs	High-capacity devices may include dedicated security hardware and/or are able to perform intensive computation. They are able to provide additional security mechanisms to protect the other devices on the HAN (for example perform key generation or network scan)

More details on technologies used in Smart Home can be found in **Annex A: “Additional details on Smart Home Environments.”**

¹⁰ For example <http://www.anandtech.com/show/9372/lifx-white-800-smart-bulb-capsule-review>.

¹¹ For example <https://www.nordicsemi.com/eng/News/News-releases/Product-Related-News/Noke-Bluetooth-Smart-padlock-employs-Nordic-Semiconductor-technology-to-eliminate-keys-or-combinations-and-enable-operation-from-smartphone>

2.2 Threats to Smart Home Environments

The threats to Smart Home Environments are real and apply to all devices and services as confirmed during the stocktaking phase of this study.^{12 13 14 15 16} While the presentation and categories of threats differ from analysis to analysis, outcome of this comparison showed that the content remains the same, that nearly all threats found in these sources are retained. Thus, the following threats groups are still relevant:

- **Physical attacks** arise from a well-identified attack vector (physical manipulation of devices). They might lead to various types of risks, including the categories described hereafter as *Nefarious Activity/Abuse* or *Eavesdropping/Interception/Hijacking*. A physical attack typically threatens all assets.
- **Unintentional damage (accidental)** may result from incorrect trust relationships or they may occur to insufficiently trained personnel (for administration, design, operation...). As it may impact administration capacities, the potential consequences also cover the whole spectrum of data leak, unauthorized modification or loss.
- **Disasters** and **Outages** were considered only as far as they result in a preventable denial of service for the user.
- **Damage/ Loss (IT Assets)** leads not only to disruption of service, but also possible leaks, as shown by ENISA's threat analysis. This study only addresses this from the point of view of the secure deletion of sensitive information at the end-of-life of a product, since all other aspects of this topic are not directly related to IT security.
- **Failures/ Malfunctions** are by definition one of the best entry points for an attacker and constitutes a first step of many scenarios of *Nefarious Activity/Abuse* or *Eavesdropping/Interception/Hijacking*.
- **Eavesdropping/Interception/Hijacking** as well as **Nefarious Activity/Abuse** are related to both privacy and cybersecurity threats. These two categories are what is generally regarded as a security threat. By leveraging design or implementation flaws, an attacker will compromise one or several assets, whether it means a loss of confidentiality on private data or a loss of control over a device. Most security good practices aim at mitigating these cases.
- **Legal**, as described in the ENISA documentation, this is another possible consequence of the same attacks. While a threat analysis is likely to contribute to distinguishing this case from the others, the attack vectors remain unchanged and they will not be distinguished from the point of view of good practices. While this study does not challenge these threats, there are however a few findings regarding the attack model and the risks associated with these threats. For more details, see [Section 3](#).

¹² Capgemini - *Securing the IoT Opportunity*, https://www.capgemini.com/resource-file-access/resource/pdf/securing_the_internet_of_things_opportunity_putting_cyber_security_at_the_heart_of_the_iiot.pdf

¹³ NCC Group - *Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond*

¹⁴ McAfee Labs - *Threats Report November 2014* <https://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q3-2014.pdf>

¹⁵ FTC - *Internet of Things - Privacy & Security in a Connected World*

<https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

¹⁶ Kaspersky Lab – *Surviving in an IoT-enabled world* <https://securelist.com/analysis/publications/72595/surviving-in-an-iiot-enabled-world/>

3. Key Findings

In this section we present the key findings discovered during the stocktaking and the analysis of the results of the on-line survey and interviews. These key findings also provide information on the challenges related to the current level of security of Smart Home products in relation with the good practices described above.

3.1 The need for security in Smart Home Environments is still underestimated

Smart Home raises new security concerns that are not easily shown in a traditional threat assessment.

Current privacy regulations ensure that service providers will not intentionally collect private data. Smart Home actors comply with this regulation by privacy measures on the server-side of their services, which would arguably be enough in a world where no malicious actors were present. However, the absence of protection on the device-side means that private data collection might be relatively easy to perform on targeted individuals, even by attackers with low skills.

Industry players usually give two reasons not to implement more security measures:

- Few attackers have an incentive to perform such attacks on an individual.
- This hypothetical targeted individual will, anyway, not chose a secure device over a lower-cost insecure device.

The first argument cannot be retained due to the lack of security in the context of today's Smart Home: when attacks are almost trivial to perform, attackers do not need many incentives.

The second argument assumes that an individual is able to give a financial cost to his private data. This line of thought is consistent with most risk assessment methods, which assess the relative importance of the threatened assets as a first step. When an asset is described as having a low value, it is expected that an attacker is less likely to compromise it, and that the asset owner is less likely to spend efforts on protecting it. The problem of this assumption is that in this case, the asset owner is not able to measure this value, since:

- they are not necessarily aware of *which private data* could be leaked; and
- they are not necessarily aware of *how easy* it is to obtain these data.

As an additional issue in the Smart Home context, trying to assess the value of private data is very difficult, since this value might vary widely depending on the local culture, amongst many other factors. This is apparent for example in the Mozaiq initiative¹⁷ which aims at ensuring that Smart Home data is stored and processed within Germany borders.

Moreover, attacks on Smart Home can target the weakest element to capture credentials of the HAN and elaborate more powerful attacks. For example, researchers have recovered the Wi-Fi private key from an unsecured device and could connect to the network to take control of the Smart Home.¹⁸

¹⁷ See <http://mozaiq-operations.com>

¹⁸ See http://www.theregister.co.uk/2015/10/19/bods_brew_ikettle_20_hack_plot_vulnerable_london_pots/

In any case, it is a common sense to say that home is the definition of *a private space*. If someone has a need for privacy, he will probably try to find it at home. This implies that the value of private data stored in Smart Home devices should only be defined by the users themselves. Since the users cannot define it today, this value is however set by industry players instead.

3.2 Vendors lack incentives to enhance security in Smart Home devices and services

Most security researchers in IoT describe the current state of the industry as not security minded.¹⁹ In particular, many actors are hobbyists or come from the startup domain. It is easy to estimate that it might cause issues on simple topics such as security updates, since these kind of actors:

- Might not have the culture of long-term support.
- Might not want to provide updates as long as their products live.
- Might not be aware of the importance of security update.
- Might even be hostile to third party researchers disclosing vulnerabilities...

More generally, the issue of the community culture is seen as a major obstacle to security. Our stocktaking and interviews shows however a slightly different picture: our overall analysis of weak security was confirmed by the actors themselves and generally resulted from an *intentional* market positioning.

Many interviewees were quite aware of security good practices, but were lacking incentives to implement them in their products. Few incentives exist to implement security, especially for low-cost devices. During the interview phase, all industry actors described the consumer market as cost-driven, functionality driven, with short time-to-market requirements, while security is a criterion only in business-to-business contexts.

Interviews and stocktaking have shown that many vendors are still waiting for end-users to ask for more security. The consumer market is seen as being mainly cost-driven, with:

- An increasing awareness of privacy issues.
- A very limited awareness of cybersecurity issues.

Some vendors are voluntarily implementing security, so as to protect the company image in case of an attack. Cost and innovation are however competing with security: except for Cloud services or smartcard providers, many actors see certification as an expensive marketing tool. However, security-aware actors share the idea that legislation, and a mandatory certification scheme, could be the only incentive able to counterbalance the time-to-market pressure, while maintaining equality amongst actors on European markets.

Effective implementation of security measures is usually found in actors who target both business-to-business and consumer markets, as the need is generally expressed by business customers.

3.3 Smart Home devices and services implement few security measures

As a consequence of the previous finding, it appears that many devices or services implement few security measures.

When following the list of good practices of Sections 4 to 7, it appears that the only features implemented today are:

¹⁹ See The Internet of Fails Where IoT Has Gone Wrong and How We're Making It Right

- Development security measures (often limited to quality control measures; in some cases, dedicated security testing is performed in a very short timeframe, such as 3-4 days campaigns)
- In terms of security functions:
 - Security audit trails (generally not protected and more used as “log files” than audit trails).
 - Secure communications (but usual good practices such as certificate pinning are ignored when using standards such as TLS).
 - Cryptographic support (generally only found in high-capacity devices such as gateways; in some cases, vulnerable cryptography is used, as shown in the OMA vulnerability cases).²⁰
 - privacy protection (mainly addressed on the remote service side, while user data are generally not protected on devices).
 - authentication (often not implemented for local network communications, and strong password policies are not always available).
 - very limited self-protection and hardening measures.
- In terms of integration in the HAN:
 - Trust relationships (albeit often weak ones, such as vulnerable pairing, or usage of trust elements without a capacity to revocation or renewal).
- In terms of usage until the end-of-life:
 - Limited operational security and maintenance.

3.4 Smart Home Environments result in new security challenges

Actors coming from the world of IoT might face new security challenges in Smart Home Environments:

- Devices will have to meet higher privacy expectations than in usual IoT devices. These specifics lead to increased privacy risks for users, while the cost of keeping data safe might be too high for industry players. The Data Protection Directive²¹ (which may soon be superseded by the General Data Protection Regulation)²² addresses general privacy protection, but might not be suitable to prevent such privacy violations. For example, a Smart TV may cause several privacy issues with that regard.²³ Home is by definition the place where privacy is expected to be enforced.
- Devices may integrate safety concerns that are specific to home. For example the loss of control of a thermostat, a smoke detector or a CO₂ detector might have consequences on the user safety. The CE marking implies liability for damages or injuries due to defects, but not due to security negligence.
- Vendors may integrate the fact that, when home is concerned, security attacks are not only a hypothesis but a fact to be dealt with. For example, a smart lock or safe is a security product and

²⁰ See Structural Weaknesses in the Open Smart Grid Protocol and Dumb Crypto in Smart Grids: Practical Cryptanalysis of the Open Smart Grid Protocol

²¹ See “Directive 95/46/EC” and its amendment “Regulation (EC) No 1882/2003”. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012>

²² See “COM/2012/011 final - 2012/0011 (COD) - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”. <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011>

²³ Even smartphones, that raise many privacy issues, would not be able to constantly and stealthily record their user: a smartphone camera does not point directly, and constantly, at the user living room; additionally, the battery drain alone would be enough to warn users that something went wrong with their device. These limitations however do not apply to a Smart TV, which causes much more privacy issues with that regard, as explained in “The Outer Limits: Hacking the Samsung Smart TV” by Aaron Grattafiori and Josh Yavor, and “Hacking, surveilling, and deceiving victims on Smart TV” by Seung-Jin Lee and Seung-Joo Kim

must be designed to sustain a cybersecurity attack. Companies selling security devices are often unaware that the “smart” part of the device can be easily compromised and rely too much on the physical part of the device.²⁴

3.5 IoT vulnerable “building blocks” cause vulnerabilities to be shared at large scale

IoT in general provides a very large ecosystem of hardware, operating systems, software and services upon which vendors can build solutions.

Many vendors are now able to integrate solutions easily, by using existing “building blocks.” But if these blocks have security flaws, these flaws will be present on all the solutions that use them.

The situation is summed up by researchers in a few sentences: *Your vendor may be leveraging six other vendors. Where’s your data going once it enters that IoT device? Who has access to your network via proxy connections?*²⁵

Several issues directly come from this situation:

- Developers do not necessarily know which frameworks and APIs are useful or vulnerable. While this is sometimes described as a lack of expertise from the developers, this is actually more probably related to the sheer number of third-party and open-source components available. This is already an issue in many domains.²⁶ A whitelisting approach might help vendors in the process of selecting secure third-party or open-source APIs.
- Vendors may be locked in third-party operating systems and applications, and not be able to patch or migrate to other solutions in cases of vulnerabilities.
- Many devices share the same third-party services or components, thus sharing their potential vulnerabilities. There is at that time no easy means:
 - To detect who are the providers of all the components and services that are integrated in a given product, and
 - To select suppliers based on security requirements.

3.6 IoT pervasiveness and dynamicity

IoT devices in general are pervasive and dynamically interconnected.²⁷ This has several consequences:

- It increases the attack surface on a given device (which may be attacked from several sources: devices, social networks, other online services...)
- It increases the nuisance potential of a device after it has been compromised (which may be connected to many other devices).
- It increases the combinations between devices and services, leading to interoperability issues (for example unintentional denial of services due to badly implemented bandwidth usage). Such issues are not security issues but may be used to investigate vulnerabilities or leverage attacks.

²⁴ See for example <https://www.defcon.org/html/defcon-23/dc-23-speakers.html#Petro>

²⁵ See The Internet of Fails Where IoT Has Gone Wrong and How We’re Making It Right

²⁶ See e.g Executive summary of the Opinion of the European Data Protection Supervisor on the Commission’s Communication on *Unleashing the potential of cloud computing in Europe* 2013/C 253/03, where the “key action 1” is “cutting through the jungle of standards”

²⁷ See The Internet of Fails Where IoT Has Gone Wrong and How We’re Making It Right

Smart Home adds a level of dynamicity, since nodes can enter or exit several kinds of networks dynamically:²⁸

- Mobile networks and internet (WAN, LPWAN).
- Virtual networks of a service provider (different identical devices and the corresponding cloud services or device management services).
- Home area network (several different devices in a single user network).

The integration of all the devices grows more and more complex due to the number of devices and their capacities to dynamically interact (researchers use the example of the If-This-Then-That mobile application, which triggers Smart Home devices behaviour on events coming from other devices, social networks, and so on).

3.7 IoT brings new constraints on security

The configurations of some devices (typically home automation sensors) are too weak to implement strong protections. This is due to not only the hardware or the device connectivity, but also the lack of identified security standards dedicated for these use cases (weak CPUs, limited memory, low bandwidth, battery usage, etc.)

Interaction with vendors show that many of them are confident in the technology to solve these issues. Hardware gets more powerful year after year. It should solve the present limitations in terms of security, even in small devices such as sensors. The main perceived barrier is the bandwidth, when using low-power networks.

²⁸ See for example IoT-A - D4.2 - Concepts and Solutions for Privacy and Security in the Resilient Infrastructure

4. Good practices for a Secure Smart Home Environment

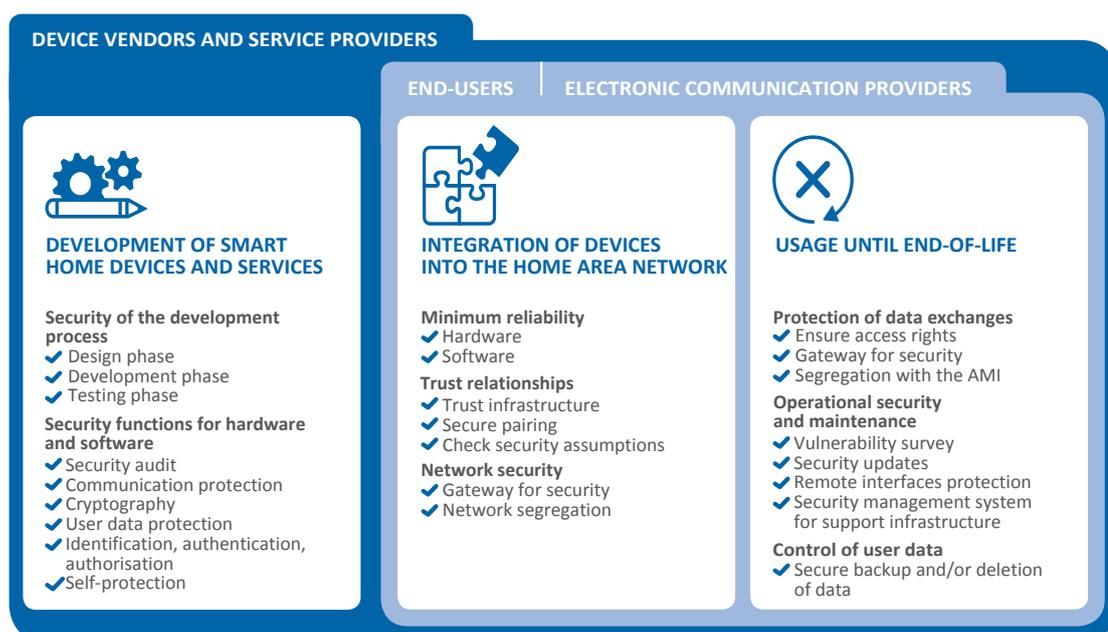
This study provides a detailed list of security “good practices” to mitigate the threats identified in Smart Home Environment. We identify different types of good practices that range from basic security hygiene to dedicated countermeasures against given threats, for different types and classes of devices as well as for associated remote services.

The list can be utilised by stakeholders as a companion to their risk assessment, either to evaluate the current level of security or to enhance it with new security measures. For that purpose, this study highlights the application of good practices to the different classes of devices and services. This list should be interpreted as an informative statement.

The good practices are presented according to the devices and services lifecycle, as well as to the stakeholder to which they apply as presented in Figure 3. These good practices are separated into the three phases of the lifecycle of devices and services:

- 1. Development of Smart Home devices and services** by device vendors and service providers. During this phase, the vendors and service providers define the requirements of the product, design, develop and test the product. The associated good practices are presented in [Section 5](#).
- 2. Integration of devices** by the end-user into his Home Area Network. During this phase, the end-user configures and connects its Smart Home device to its HAN, potentially with support of the device vendor, the service provider, or the electronic communication provider. The associated good practices are presented in [Section 6](#).
- 3. Usage of the devices and services until their end-of-life.** Apart from direct and local interactions with his device, the end-user may also request support from the vendor and use on-line services related to the device through various communication channels. Thus this phase may imply interactions with the device vendor, the service provider, or the electronic communication provider for usage and decommission. The associated good practices are presented in [Section 7](#).

Figure 3: Good practices within the Smart Home lifecycle and their applicability to stakeholders



5. Good practices for the development of Smart Home devices and services

This section describes the good practices related to the development of Smart Home devices and services. These good practices consist of two different sets:

- Security “good practices” for the development process of Smart Home devices and services.
- Security functions that are considered good practices. These security functions address the devices themselves and their interfaces with web services and mobile applications.

5.1 Security of the development process

The development process comprises the design phase, the development phase and the testing phase. For each phase, several good practices are highlighted.

5.1.1 Design phase

Security concerns must be taken into account in the early phases of the product or service lifecycle. As a general rule, the security architecture of a solution must be defined and documented early. This is the practical implementation of the often-used *security by design* requirement.

At the design level, several aspects can be recommended to vendors as well as service providers, as described in existing guidance.²⁹

Use defence in depth³⁰

Applies to remote services, class 1 devices and higher

Designers should assume that their security measures will be compromised at some point – and they should therefore provide redundancy by the means of layered security measures. It also means that error and attack scenarios should be taken into account during the design (not limiting the design to nominal cases).

Separate security functions from other functions

Applies to remote services, class 1 devices and higher

Consequently security functions should have clear and limited interfaces to the “non-secure” functionality. It enables to clarify interfaces between the “secure” and “non-secure” functions, thus limiting the design errors that might arise. It enables to separate development teams and focus the task of security experts only on secure parts.

When “secure” and “non-secure” parts are not necessarily easy to distinguish, using a modular design gives an assurance to separate functions and clarify interfaces.

All “secure” and “non-secure” parts should be reviewed from a security point of view, since many vulnerabilities can originate from “non-secure” parts such as memory management or string formatting.

²⁹ Security of Things: An Implementers’ Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group

³⁰ See for example https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Make assumptions for the security requirements explicit

Applies to remote services, class 1 devices and higher

The design stage should clearly explain the assumptions for the security requirements. Such assumptions include:

- Limitations in the usage of the device (for example, a given device might need ZigBee connectivity to transmit security alarms, implying that it will not be able to send alarms when deployed behind a very thick wall)
- Assumed properties of the environment (for example, assuming that the certification authorities in the certificate store are all trusted and not compromised)

Assumed properties of cryptographic properties (for example, assuming that a given algorithm and key size are sufficient for a given task).

Consider third-party review by security specialists for developers with limited security experience

Applies to remote services, class 1 devices and higher

An independent third-party review is recommended for the whole design; it is deemed to be crucial especially for cryptography, in order to select the appropriate algorithms and associated functions, and know-how to implement or configure them correctly. This review should be a mandatory step during the design stage, since cryptographic operations might put resource conditions that have a significant impact on components procurement. Such a review is also absolutely crucial for *system security*, i.e. considering the security elements in the whole usage context, in order to avoid inconsistencies and design flaws (for example sensitive elements could be safely stored but allowed to leak by other channels such as error messages)

Prepare user interactions with the products or services

Applies to remote services, class 0 devices and higher

Developers must prototype the user interface as soon as possible in order to identify ways to help users on security issues.

Interactions with the user can happen in many forms and the security impact of these interactions have to be carefully planned. The US Federal Trade Commission (FTC) reminds that it does not only concern setup wizards, admin dashboards or external signals (LEDs/alarms/icons...), but also sign-up procedures and information emails/or SMS.³¹

5.1.2 Development phase

The importance of development of the product for security is two-fold. It is during this step that security functions are used or implemented to satisfy the security requirements from the design phase and also that programming errors may introduce security vulnerabilities.

For that purpose, actors involved in product and service development use security-enhancing tools, and ensure training and awareness of their developers.

³¹ See FTC Careful connections and FTC - Internet of Things - Privacy & Security in a Connected World for data collection

Use configuration management tools, and leverage upon development environments such as compilers or static analysers

Applies to remote services, class 1 devices and higher

The source code (for hardware developers, this may include HDL files) should be managed according to a sound configuration management process, in order to be able to identify versions, responsibilities of changes, and so on.

Static code analysis should be used to gain security assurance on the code (by identifying potential vulnerabilities), as well as quality assurance. Static code analysis is usually based on automatic tools.³²

Compiler security options must be used when native code is used.³³

Take security into account when choosing your programming language; when available, leverage upon the operating system security functions

Applies to remote services, class 1 devices and higher

Some programming languages offer memory management capacities. The use of such “managed code” instead of native code should be considered from a security point of view, but it must be considered carefully. The usage of “Managed code” in place of native code has both benefit and costs:

- Benefit: Managed code can reduce the risk of vulnerabilities due to memory allocation, and the need for memory management guidelines.
- Cost: Managed code can make it harder to really control the erasure of elements in memory, so native code might be more appropriate when processing key material, for example. When used for security functions, managed code is also easier for an attacker to decompile and understand.
- Cost: any vulnerability in the shared memory management capacities lead to a single point of failure³⁴ so the runtime associated with the managed code must be kept up-to-date.

The good practice generally consists of using both “managed code” and native code for different purposes, and limit native code to parts where a low level of control over security elements is needed.

Operating system security options must be used with the associated compiler options.³⁵

Use standard, secure frameworks or stacks whenever possible – do not redevelop security functions

Applies to remote services, class 1 devices and higher

For example in cryptography, existing libraries must be used: redevelopment is widely considered as a bad practice.

Of course, existing libraries might also have flaws, and there is no simple criterion to assess whether a given library should be trusted or not. Several information should be used for this purpose:

³² See Internet of things research study, HP 2014. Licensed tools exist for static analysis, but several free alternatives also provide valuable information, such as Clang or Findbugs

³³ Options vary depending on the language, compiler and target OS; to see what kind of protection they can provide, see for example <https://wiki.debian.org/Hardening> (gcc under Debian).

³⁴ See for example <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313>

³⁵ ASLR or CFI are examples of such options (see <http://pax.grsecurity.net/docs/aslr.txt> and <http://clang.lvm.org/docs/ControlFlowIntegrity.html>). Other mechanisms exist, a recent albeit controversial example being RASP (runtime application self-protection)

- Does it implement standard mechanisms? (e.g., “standard” mechanisms may refer to mechanisms approved by the ISO/IEC JTC 1/SC 27 subcommittee, including its workgroup 2 for cryptography. It may also refer to mechanisms approved by national cybersecurity agencies).
- Is it widely used? (even if this is no definitive guarantee of security, a widely used library such as OpenSSL should probably be preferred to a brand new library that has been developed a few weeks ago).
- Has it been audited? (for example an independent audit was performed on TrueCrypt to assess its resistance to cryptanalysis).³⁶
- Has it been verified? (for example some libraries underwent government or proprietary certification programs such as FIPS 140-2, which give an additional assurance).

Ensure team training and awareness

Applies to remote services, class 1 devices and higher

It is necessary to make sure that the teams in charge of security are skilled enough:

- Secure programming guidelines should be used and regularly updated whenever flaws are found in the product. An example of such guideline can be found at OWASP.³⁷
- Security training must be in place for the developers contributing to critical parts.
- Security training should also be in place for all the other developers/testers, as many security flaws can occur in “non-secure” parts (for example the lack of input validation in user interfaces).

5.1.3 Testing phase

Testing the compliance of a product, or service, against its specifications, is required to give assurance of its correct behaviour. Such tests should not only focus on the “nominal” behaviour, but also cover a robust error handling and fault tolerance. This will reduce the opportunity for an attacker to exploit vulnerabilities, for example improper input validation.

However, even to claim a basic level of robustness against attacks, compliance testing is not enough. For example, a simple error case test of a web service input fields will not be able to detect a potential vulnerability to a script injection. Vulnerability assessment and testing provide the appropriate assurance against an attack, because they actually *consist in simulating or even performing such attacks*.

Test the compliance of security functions

Applies to remote services, class 1 devices and higher

Tests must demonstrate that the security behaviour of the product or service is effectively implemented.

Patches must be validated (for example if patches are applied to usual open source libraries, Linux kernel, OpenSSL...).

Automated unit tests and continuous integration should be considered.³⁸

Automated and manual test plans must be updated according to the findings of the security audits.

³⁶ See <https://opencryptoaudit.org/>

³⁷ <https://www.owasp.org>

³⁸ ASLR or CFI are examples of such options (see <http://pax.grsecurity.net/docs/aslr.txt> and <http://clang.llvm.org/docs/ControlFlowIntegrity.html>). Other mechanisms exist, a recent albeit controversial example being RASP (runtime application self-protection)

Perform additional security audits and penetration testing

Applies to remote services, class 1 devices and higher

Compliance testing should be completed by dedicated security audits or penetration testing.

Skilled experts should simulate attacks and try to circumvent or weaken the product or service security functions. The scope may vary depending on the target product but should at least include:

- A design and code review for critical parts (notably cryptography) and for the system as a whole.
- A configuration review of the product or infrastructure.
- A network scan (for infrastructures).
- A radio frequency audit (if applicable).
- An assessment of the public vulnerabilities that might impact the product.
- Penetration testing.

Perform a privacy assessment

Applies to remote services, class 1 devices and higher

Conduct an analysis of the design and implementation of the product or service, to ensure that private data is correctly processed with regard to European regulations.

The approach consisting in implementing privacy protections from the design phase has led to the often used notion of “privacy by design”, which may appear confusing to several vendors, since it might lead to think that privacy can be obtained by the application of simple design patterns or rules. Quite the contrary, this approach is more easily implemented by performing an *independent assessment* of the design.

Such assessment can take multiple forms but is often called a Privacy Impact Assessment. This activity can typically be performed by the developer itself or by a third-party, which guarantees both skills and independence for the assessment.

As a good example of such approach, the BSI issued in 2011 a guidance in English:

- A Privacy Impact Assessment Guideline.³⁹
- A Privacy Impact Assessment Guideline for RFID applications.³⁹

Vendors should also be aware that their national privacy agencies, such as the French CNIL,⁴⁰ might have published guidance for privacy assessment in their own language.

³⁹ See BSI - Privacy Impact Assessment Guideline (Kurzfassung),

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfassung.pdf?__blob=publicationFile

⁴⁰ See CNIL – Guides pratiques, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-1-Methode.pdf, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-2-Outillage.pdf and http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-3-BonnesPratiques.pdf

5.2 Security functions for hardware and software

This section describes security functions, or requirements, which are considered good practices for devices as well as mobile applications or services.

These requirements use categories loosely adapted from the Common Criteria⁴¹ security certification standard. These categories are:

- **Security audit:** security events must be logged, and users should be notified whenever needed.
- **Communication protection:** communication should be protected against disclosure, modification, replay and denial of service.
- **Cryptography:** Confidentiality, integrity and authenticity must be protected by using strong and standard cryptography. Keys must be managed securely, and the use of a trust infrastructure (such as PKI) is encouraged.
- **User data protection:** the integrity, confidentiality and authenticity of user data must be protected. Confidentiality protection must be defined with regards to privacy issues.
- **Identification, authentication, authorization:** strong authentication methods must be used, as well as access control mechanisms. Passwords and sessions should be managed accordingly.
- **Self-protection:** HW and SW self-protection measures should be in place to protect previous security functions. Data used to enforce these security functions should be protected, and hardening should be used to reduce the attack surface.

5.2.1 Security audit

Security audit aims at enabling logging, audit and forensic and at providing user notification.

Log security events

Applies to remote services, class 1 devices and higher

Security events must be logged⁴² and access to the logs must be documented and protected from disclosure to unauthorized users.

Logs are also needed for device integration. Typically, HW suppliers must give possibility for their customers to understand security events happening at the HW level.

However logs may also give information to an attacker, which is a serious security drawback. For this reason, the audit trail must be protected:

- Logs should be anonymous (see [good practices on User data protection](#) for anonymity measures).
- Avoid logging information that would give useful information to an attacker.⁴³
- Access control mechanisms should limit the access to the logs (see [good practices on Identification, authentication, authorisation](#)).
- When sent to a remote system, logs should be protected by cryptographic mechanisms (see good practices on [Cryptography](#)).

⁴¹ <http://www.commoncriteriaportal.org>

⁴² See Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group and see OWASP I8 | Insufficient Security Configurability

⁴³ For example the stack trace in Java, or the memory current status

Notifications should be easy to understand and help users find a remediation or workaround

Applies to remote services, class 1 devices and higher

HW and embedded systems should provide clear error data that can be leveraged upon by the SW vendors. The user must be notified in case of security errors, updates or compromised data⁴⁴ in a device or service they use.

In particular, users must be notified in the case of security events⁴⁵. Notification might vary greatly depending on the type of software considered. Mobile applications notification, messaging such as SMS or e-mail, hardware interfaces such as LEDs, dedicated error messages to a gateway...

However developers should be aware that for some functions, an excess of clarity is a valuable information for an attacker. As a common example, when a login fails, the product should not communicate to the user whether the error is due to a non-existent login or a bad login/password combination.

The optimal balance between *not enough* or *too much* clarity is to be assessed during dedicated security testing (see good practices for the **Testing phase**).

5.2.2 Communication protection

The protection of communications aims at protecting against disclosure, modification, replay and Denial of Service. Moreover, the protection of communications shall also protect authentication and associated mechanisms.

Protect all communication against disclosure, modification and replay

Applies to remote services, class 1 devices and higher

Provide end-to-end protection in confidentiality and integrity. Use protocols that resist replay attacks. Favour methods providing forward secrecy whenever possible. This should be true even for the communication of already encrypted data.⁴⁶

Encryption must cover not only WAN traffic (Internet and LPWAN traffic), but also local networks.⁴⁷

Many protocols use both transport layer and applicative layer protection. The need for applicative layer protection comes from end-to-end protection needs: the transport layer could be exposed if different transport technologies are used during the transmission, therefore needing a dedicated protection:

- In TCP communications, the latest version of TLS⁴⁸ is the default choice for securing the transport layer; DTLS is an equivalent of TLS for UDP communications.
- Applicative layer can be protected by recognized cryptographic means, so as to protect confidentiality and integrity of the payload.

Note that manufacturers and service providers are expected to manage the security of their cryptographic keys and certificates used by their devices and services (see **good practices on Cryptography**).

⁴⁴ See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

⁴⁵ see OWASP I8 | Insufficient Security Configurability

⁴⁶ See OWASP I9 | Insecure Software/Firmware, or Symantec Insecurity in the Internet of things, March 12, 2015

⁴⁷ See OWASP I4 | Lack of Transport Encryption

⁴⁸ Or DTLS for datagram communication such as UDP

Mitigate vulnerabilities or limitations of standard security library

Applies to remote services, class 1 devices and higher

Using a standard security library does not mean that the product will automatically be secure. Developers must be aware of the vulnerabilities (due to a flawed implementation) and limitations (vulnerability of the protocol itself) of the third-party components they use. They should mitigate them whenever possible by performing patching and by securing the configuration of the communication stacks, which might typically include:

- Bluetooth.⁴⁹
- 6LowPAN/ZigBee/802.15.4.⁵⁰
- Wi-Fi.⁵¹
- TLS or DTLS.⁵²

Regarding Patching: Communication protection protocols are often implemented by using third-party or open-source libraries. They all need frequent patching: vulnerabilities are regularly found in all these implementations, even those considered as “industry standard.” Communications protection work only as long as firmware updates are available and applied to fix vulnerabilities. See [good practices on Operational security and maintenance](#) for more details on security updates.

Regarding Configuration: Due to the existence of vulnerabilities in frequently used protocol implementations, configuration of the library is a significant part of the security functionality. Developers should in particular be vigilant to the configuration of cipher suite negotiation and key sizes: allowing weak cipher suites provides an entry point for attacks aiming at downgrading the level of security of the exchanges⁵³. See [good practices on Self-protection](#) for more details on hardening. Amongst many examples, here are two recent vulnerabilities:

- OpenSSL libraries that were compiled to work with heartbeats were vulnerable to the Heartbleed bug.⁵⁴
- ZigBee allows some flexibility, thus potential implementation or configuration flaws.⁵⁵

⁴⁹ See the example of Bluetooth, including Bluetooth 4.0, in *Guide to Bluetooth Security - Recommendations of the National Institute of Standards and Technology - John Padgett, Karen Scarfone, Lily Chen*

⁵⁰ See for examples replay attacks, or attacks on key provisioning in KillerBee: Practical ZigBee Exploitation Framework or “Wireless Hacking and the Kinetic World”, by Joshua Wright. 6LowPAN was also successfully attacked, see for example Hacking into Internet Connected Light Bulbs, Alex Chapman, 04 July 2014

⁵¹ See for instance attacks on WEP <http://eprint.iacr.org/2007/120.pdf>, WPS PIN vulnerability <https://www.kb.cert.org/vuls/id/723755> or the Pixie Dust attack on WPS https://passwordscon.org/wp-content/uploads/2014/08/Dominique_Bongard.pdf

⁵² SSL and TLS have a long history of security vulnerabilities (see <https://tools.ietf.org/html/rfc7457>). TLS and DTLS share some vulnerabilities, for example CVE-2013-0169, also known as *Lucky13*

⁵³ See for example CVE-2015-0204 at <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204>

⁵⁴ See “How can OpenSSL be fixed ?” at <http://heartbleed.com/>

⁵⁵ See http://cognosec.com/zigbee_exploited_8F_Ca9.pdf

Protect communications against denial of service

Applies to remote services, class 1 devices and higher

Consider denial of service as a usual threat to communication infrastructures.⁵⁶

This threat should be addressed from the design phase of the infrastructures.

On this topic, this study encourages the vendors and service providers to read the *ENISA Internet Infrastructure Threat Landscape* (for network components)⁵⁷ or the *GSMA IoT Device Connection Efficiency Guidelines*.⁵⁸

5.2.3 Cryptography

Cryptography aims at many protection measures to protect data confidentiality and integrity rely on cryptographic functions. In a broad definition, cryptography support for security must include user's protection and authentication, data protection and the cryptographic infrastructure. For example, such a support may implement:

- For authentication primitives:
 - user/entity authentication;
 - message authentication and integrity.
- For data protection:
 - symmetric or asymmetric encryption;
 - hash functions;
 - digital signature.
- For cryptographic infrastructure:
 - random number generation;
 - key management.

We identify hereafter four main considerations for cryptography:

- Use strong and standard cryptography, including random number generation.
- Use hardware-accelerated cryptography with care.
- Manage and provision keys securely.
- Use of trust and reputation infrastructures.

Do not create proprietary cryptographic schemes, but use state-of-the-art standards instead.⁵⁹ Even a home-brewed implementation of a standard is not a good practice when standard implementations are available.

Applies to remote services, class 1 devices and higher

If needed, consider getting advice from security experts or your national cybersecurity agency.⁶⁰ If no recommendations exist for vendors at a national level, ENISA recommendations should be considered as a

⁵⁶ See OWASP I3 | Insecure Network Services

⁵⁷ See <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure>

⁵⁸ <http://www.gsma.com/connectedliving/gsma-iot-device-connection-efficiency-guidelines/>

⁵⁹ See for example see Symantec Insecurity in the Internet of things, March 12, 2015 or Careful connections by FTC

⁶⁰ This study will not delve into the detailed requirements for cryptographic algorithms or acceptable keys sizes, since most of national cybersecurity agencies already provide consistent guidance on this topic

reference.⁶¹ This applies also to random number generation, which is a critical part of the cryptographic support. A possible recommendation would be the use of cryptographically secure pseudorandom number generators.⁶²

Rely on an expert in cryptography for interfacing with HW accelerated cryptography or secure elements, or even using or configuring a standard implementation.

Applies to remote services, class 1 devices and higher

These tasks are difficult for most of developers. If not properly done, the security might be heavily reduced or even completely suppressed. This part should be performed by an expert in cryptography or at least a third-party code review should be performed to ensure that HW or a standard implementation of cryptography is properly used.

When designing or procuring HW, pay attention to the requirements of cryptography in terms of CPU, memory and bandwidth and their impacts on battery.

Applies to class 1 devices and higher

On high-capacity devices, consider using dedicated hardware security modules.

Be aware of limitations of HW-based cryptography solutions and choose wisely whether a SW or HW solution is needed for the given context.

Applies to class 1 devices and higher

HW-based cryptography solutions may help avoiding the incorrect implementation of cryptographic algorithms by software vendors, as well the coexistence of multiple implementations of the same algorithms. They eventually provide implementations that are more resource-efficient.

Low-end HW might not be able to perform strong cryptography (due to memory and/or CPU capacities for example); consider using Elliptic Curve Cryptography over RSA, especially for CPU- and memory-limited devices.⁶³

Choosing HW accelerated cryptography means that a reasonable assurance must be obtained on the quality of the HW implementation, since “bad cryptography” on HW will be leveraged on all the SW using these functions.⁶⁴

Regarding true and pseudo-random number:

- As a general rule, a true random number should be used for key generation, but may not be required for salts, initialization vectors etc., where a cryptographically secure pseudo-random number may be sufficient. One may argue that using a cryptographically secure software pseudorandom number generator is more secure than a badly implemented hardware “true random number generator.”
- When using hardware claiming a “true random”, developers should consider using strong post-processing functions. The functions used for that purpose are typically block encryption or hash functions.

⁶¹ See <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014>

⁶² See examples in <http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf>

⁶³ Symantec Insecurity in the Internet of things, March 12, 2015

⁶⁴ It should be reminded that this study does not consider side-channel attacks, which would require further development on the topic of hardware cryptography.

- Some standard groups for Smart Home address this point by always requiring a true random, *and compliance of this random to given test vectors*.⁶⁵

More details on the different categories of random generators can be found in references from national cybersecurity agencies.⁶⁶

Vendors could consider HW-based cryptography as a criterion for HW procurement (Smart Home devices or network HW for cloud infrastructures). In this case, HW-based cryptography must be used according to the HW guidelines that will describe how to securely use the HW.

If needed, consider getting advice from security experts or your national cybersecurity agency.

Manage keys securely

Applies to remote services, class 1 devices and higher

As a general rule, cryptographic keys should be securely generated, distributed (or provisioned), used, stored, and deleted (including revocation).

Badly implemented key management can introduce vulnerabilities that are often exploited, even in Smart Home devices.⁶⁷

Smart Home introduces a few new specifics: Smart Home incorporates technologies coming from machine-to-machine technologies without direct user interface (for example surveillance cameras). It has consequences in terms of key provisioning for at least two reasons:

- Devices without direct user interfaces are particularly vulnerable to attacks on a PKI (loss of certificates...). While users of a PC can easily delete or install certificates, such devices rely mostly on remote administration, and sometimes do not even allow end-users to perform such administration tasks. For this reason, Smart Home vendors should consider very carefully the revocation mechanisms associated with their devices, and the end-user means to easily fix issues of that kind.
- Industry players introduced the notion of remote provisioning for mobile communication.⁶⁸ While keys are loaded in SIM cards in protected environment, the “embedded UICCs” rely on remote subscription management systems to obtain key material. The protection of these exchanges is consequently critical and must be assessed accordingly by manufacturers and vendors. Should the keys be leaked, the user *and* the vendors could be at risk in many ways (loss of control over the device, eavesdropping, credential theft, cloning etc.). More generally, the notion of confidential key agreement must be considered in IoT in general, and Smart Home in particular.

As a general practice, Smart Home devices should leverage upon their user interfaces to mitigate the risks caused by key management constraints. Key management must be transparent to the user. It shall only be necessary for the first-time peering. For that purpose, it is important to provide user-friendly mechanisms

⁶⁵ See for example the Home Gateway Initiative: <http://www.homegatewayinitiative.org/publis/RD039-Req-for-Wireless-home-area-networks.pdf>

⁶⁶ See *A proposal for: Functionality classes for random number generators, Version 2.0*, 18 September 2011

⁶⁷ See for example *Making Smart Locks Smarter (aka. Hacking the August Smart Lock)* or *the Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right* and *LIFX vulnerability*

⁶⁸ See for example *GSMA remote provisioning architecture* and *Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond*, NCC group

to ensure authentication. For example, a visual graphic interface can be used to authenticate devices, with a QRCode.⁶⁹

If needed, consider getting advice from security experts or your national cybersecurity agency.⁷⁰

Use trust and reputation infrastructures

Applies to remote services, class 1 devices and higher

See good practices presented in **Section 6** on the Integration of devices in the Home Area Network.

5.2.4 User data protection

The user data protection includes:

- The notion of privacy/confidentiality.
- The notion of integrity and authenticity (for example related to theft of loss of control over the devices).

For that purpose, it is important to define privacy/confidentiality protection measures before they are implemented in devices and services.

Identify personal data

Applies to remote services, class 1 devices and higher

The interpretation of privacy protection raises many issues, one of them being to successfully identify what can be considered a personal data. The definition according to the EU Data Protection Directive 95/46/EC⁷¹ includes data *relating to an identified or identifiable person*.

In the case of the Smart Home devices, however, it may be safe to assume that *any data* related to the user activity is somehow personal, since the location of this activity can be linked to an occupant of the user home. This last approach will have to be continued throughout the whole product or service lifecycle.

Metadata should be considered as personal data by default, since they are subject to the same threats.⁷²

Consider getting advice from your national data protection agency.

Implement transparency measures

Applies to remote services, class 1 devices and higher

The interactions with the user (which should not be limited to the *Terms and conditions*)⁷³ enable to cover the legal transparency requirements

The service or device provider must communicate:

- The provider's name and address.

⁶⁹ See SQRL Authentication. <https://en.wikipedia.org/wiki/SQRL>

⁷⁰ This study will not delve into the detailed requirements for cryptographic algorithms or acceptable keys sizes, since national cybersecurity agencies already provide consistent guidance on this topic

⁷¹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

⁷² See <http://www.lifehacker.com.au/2015/02/why-the-internet-of-things-is-a-problem-for-metadata-retention/>

⁷³ While the Terms and Conditions are a practical support for the vendors, many actors consider that this cannot be considered a good practice. In particular, the user may be lost in a barely-legible legalese instead of being able to make informed choices regarding their privacy. The US FTC gives recommendations on this topic, for example using other supports such as registration emails.

- What data is collected, in layman terms.
- The purpose of processing,⁷⁴ explaining notably why the processing is necessary for the performance, or why it is necessary for compliance with a legal obligation.
- The recipients of the data.
- How the user can:
 - Access all data processed about him.
 - Require the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules.
- And all other information required to ensure the processing is fair.

The service or device provider must require the consent of the user (or “data subject”).

On top of legal requirements, actors might also consider:

- Defining a strict opt-in policy.⁷⁵
- Enabling rectification, deletion or blocking of data without a reason.
- Ensuring data portability.

Design the product/service with legitimate purpose and proportionality in mind

Applies to remote services, class 1 devices and higher

The design phase of the service or product, where the details of the processing have to be assessed with regards to the explicit and legitimate purposes. The actors must ensure that themselves *and their subcontractors or suppliers*:

- Do not process user data more than needed.
- Do not pursue an illegitimate purpose with regard to user data.

As a general rule, third party components integrated in the device or third party cloud services should not access unencrypted user data unless user agreement has been obtained. Access control or anonymity/pseudonymity measures gives assurance that user data is not accessed by these third parties.

Define access control, anonymity and unlinkability measures to enforce the protection of private data

Applies to remote services, class 1 devices and higher

These measures intend to protect confidentiality and integrity are typically:

- Access control measures:
 - As a general rule, access to sensitive data should be controlled (see [good practices on Identification, authentication, authorisation](#)).
 - For web services and devices including virtualization, access control could be completed by data isolation (see [good practices on Self-protection](#)).
- Anonymity measures:

⁷⁴ The European directive also includes cases where “processing is necessary in order to protect the vital interests of the data subject”, or “for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.” This topic could be typically related to the use cases of smoke or CO₂ detectors.

⁷⁵ See for example OWASP I5 | Privacy Concerns

- “one-way” or “non-reversible” measures such as truncation⁷⁶ or a hash function.⁷⁷
- reversible such as encryption⁷⁸ (see [good practices on Cryptography](#)). Encrypted storage can also address authenticity or integrity of user data if combined with the right mechanisms (for example AES-GCM).
- Pseudonymity and mainly unlinkability measures, such as ensuring that data is not correlated.

The typical example is ensuring that the key used to browse the “customer database” is not the same as the key used to browse the “usage analytics database.” However the situation is more complicated in practice: in the case of Smart Home, for example, network locator is a critical factor of linkability and should be taken into account accordingly.⁷⁹ Vendors should also be aware, that unlinkability can also:

- Cause trust issues⁸⁰ and reduce attack mitigation capabilities (for example if a user cannot be notified that their device is compromised).
- Cause a conflict with other legal requirements.

There is no one-size-fits-all good practice to balance unlinkability against other desired properties. The right balance must be defined during the design stage by examining the associated risks.

5.2.5 Identification, authentication, authorisation

Use mutual authentication for remote communication

Applies to remote services, class 2 devices and higher

The objective is to perform strong authentication before granting access to sensitive functions or data.

Devices or users connecting to a server must be able to authenticate the server. Reciprocally, servers must be able to authenticate clients and users.

Mutual authentication⁸¹ consists in demonstrating cryptographically to both the client and the server that they are communicating with the expected party.

Mutual authentication is generally supported by Public Key Infrastructures (PKI) and certificates. The use of such infrastructure components is supported by protocols such as TLS. However using methods such as these does not grant a secure mutual authentication, unless:

- There is a certificate for *both the server and the client*.
- Certificates are properly validated (ruling out, for example, the use of self-signed certificates).
- Revocation lists are verified (alternatively, interrogations to an OCSP server).

⁷⁶ Truncation is often used in the payment industry to anonymize cardholder data (see <https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>)

⁷⁷ Hash functions also have vulnerabilities (see for example https://en.wikipedia.org/wiki/Cryptographic_hash_function). As for other cryptographic operations, robust standard mechanisms should be preferred – vendors are encouraged to contact their national cybersecurity agency if needed.

⁷⁸ See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right, OWASP I5 | Privacy Concerns and OWASP I10 | Poor Physical Security

⁷⁹ See IoT-A - D4.2 - Concepts and Solutions for Privacy and Security in the Resilient Infrastructure

⁸⁰ See for example IoT-A - D1.5 - Final architectural reference model for the IoT v3.0

⁸¹ See Symantec Insecurity in the Internet of things, March 12, 2015

- *All services* require this authentication step.⁸² Which also means that even private URLs accessible on a device must require authentication.⁸³
- Certificate pinning is used.⁸⁴

As a side note, it must be noted that certificate pinning does not eliminate the need for certificate validation. For example, the pinned certificate can be an intermediate or root Certificate Authority (CA) – which means that the end certificate still has to be verified against the CAs.

Use multi-factor authentication for user authentication

Applies to remote services, class 2 devices and higher

The objective is to perform strong authentication before granting access to sensitive functions or data.

Users should be authenticated by multi-factor authentication whenever possible, including for authentication to cloud services or mobile interfaces⁸⁵ as well as local administration sessions of devices.

Several methods can be used for multi-factor authentication. As an example, the NIST provides a summary of these methods.⁸⁶

Implement access control measures to separate the privileges of different users as well as the privileges of different applications

Applies to remote services, class 2 devices and higher

The objective is to control access to sensitive functions or data.

Implementing privilege levels, rings or domains is a good practice. Some platforms implement such levels in hardware. If such functions are available, vendors are advised to use them.⁸⁷ If not, operating systems already provide capacities to implement privilege control. At the firmware / software level, access control must be used to control access rights of *both applications and individuals*. In particular:

- For devices with an operating system, not all applications need to be root or be executed in kernel land.⁸⁸
- Not all individuals need to have access user data stored in the device or associated services.⁸⁹

Other measures are required at a firmware or software/applicative level:

- User accounts must be unique and separated for both local and distant services.⁹⁰

⁸² See See Home Automation Benchmarking by SYNACK, but also Making Smart Locks Smarter (aka. Hacking the August Smart Lock), The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right.

⁸³ See example of TRENDnet IP cameras vulnerability

⁸⁴ See Home Automation Benchmarking by SYNACK or Making Smart Locks Smarter (aka. Hacking the August Smart Lock). For details on Certificate pinning, see

https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning#What_Is_Pinning.3F

⁸⁵ see OWASP I2 | Insufficient Authentication/Authorization, I6 | Insecure Cloud Interface, I7 | Insecure Mobile Interface

⁸⁶ See NIST Special Publication 800-63-2 – Electronic Authentication Guideline

⁸⁷ See “Security of Things: An Implementers’ Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group”

⁸⁸ See for example “Smart TV Security - #1984 in 21st century”

⁸⁹ I5 | Privacy Concerns

⁹⁰ See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

- The device must distinguish between normal users and admin users. The latter only have access to configuration functions.⁹¹

Implement a strong password management policy

Applies to remote services, class 1 devices and higher

It is important to allow and encourage the use of strong passwords.

As it is regularly demonstrated, passwords are often a weak point, whether they are weak user passwords or weak default passwords for products internal services. Many devices use strong protection measures that are defeated by the lack of proper password management.

This concerns all possible uses of passwords: direct device interfaces such as JTAG, but also web, mobile or cloud interfaces. The usual measures are the following:

- Allow and encourage the use of strong passwords.⁹²
- Require the user to change credentials (username, password) at their first login.⁹³
- Do not use hard-coded or “default” passwords or shared passwords,⁹⁴ for instance for remote support accounts.
- Do not store/expose passwords in clear text or with weak protection.⁹⁵ Adaptive one-way functions such as PBKDF2, scrypt or bcrypt should be preferred.⁹⁶
- Use countermeasures against password guessing / account harvesting.⁹⁷ Services must be protected against:
 - Horizontal guessing (testing a small number of usual passwords on a high number of user accounts).
 - Vertical guessing (testing a high number of passwords on a single user account).
 - This typically includes lock-out and delaying measures as well as high password strength / entropy and diversification of passwords across devices. This also includes countermeasures against account discovery or other means used to exploit password recovery functions.⁹⁸
- Define options for password control. Typically, in the case of an administrator account, the default option should require strong passwords by default.^{99 100}

⁹¹ See OWASP I8 | Insufficient Security Configurability

⁹² See I2 | Insufficient Authentication/Authorization and OWASP I1 | Insecure Web Interface. See also see Symantec Insecurity in the Internet of things, March 12, 2015

⁹³ See OWASP I1 | Insecure Web Interface, OWASP I6 | Insecure Cloud Interface, OWASP I7 | Insecure Mobile Interface

⁹⁴ See Home Automation Benchmarking by SYNACK, and Careful Connections by FTC

⁹⁵ See Home Automation Benchmarking by SYNACK, also The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right. See OWASP I2 | Insufficient Authentication/Authorization See Careful Connections – FTC.

⁹⁶ See https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet. Hash functions such as MD5, SHA should not be used for password protection, and even SHA256 or SHA3 would lack the additional work factor to be efficient in a password storage context

⁹⁷ see Symantec Insecurity in the Internet of things, March 12, 2015 and Home Automation Benchmarking by SYNACK

⁹⁸ see OWASP I2 | Insufficient Authentication/Authorization

⁹⁹ See OWASP I2 | Insufficient Authentication/Authorization and OWASP I8 | Insufficient Security Configurability

¹⁰⁰ An example of policy can be found at <https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy>. Policies may vary depending on the threat analysis and dimensions (such as password length) also

- Password policies are eventually useless if the final user is not fully aware of the threats and good practices. Vendors and service providers should consider raising the awareness of their users whenever possible, for example to support the use of password managers. Examples of simple guidelines can be found in *ENISA Basic security practices regarding passwords and online identities*.¹⁰¹

Enforce session management policies to avoid session hijacking

Applies to remote services, class 2 devices and higher

Enforcing a secure session management policy also contributes to making sure that the authorized user is the one using a given session. Typically:

- Sensitive functions such as administration via web services should require re-authentication.¹⁰²
- No data should be transmitted before authorization.¹⁰³
- Strong (random) session handlers should be used to avoid replay.¹⁰⁴
- The user must know at any time if, and why, they are logged on a particular service, meaning that no passive sign-up for third party services should be performed.¹⁰⁵

5.2.6 Self-protection

Self-protection includes all measures taken to enhance the robustness of previously mentioned security functions. Developers should challenge every security function of their design, consider how they could be bypassed or weakened, and eventually implement self-protection measures. The main topics considered here are:

- **Hardware self-protection:** these measures aim at protecting the hardware against physical attacks or observation. They include tamper evidence or tamper resistance, and secure design measures.¹⁰⁶

depend on attacker's capabilities, especially the computing power, which grows constantly over time. Vendors are invited to contact their national cybersecurity agency or CERT to stay informed of the state-of-the-art.

¹⁰¹ See <http://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities>

¹⁰² See OWASP I2 | Insufficient Authentication/Authorization

¹⁰³ See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

¹⁰⁴ See for example Veracode White Paper – The Internet of Things: Security Research Study, 2015, and also The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

¹⁰⁵ See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

¹⁰⁶ Hardware protection measures are related to:

- threats that are not related to privacy, and where the user itself is the attacker (for example fraud use cases);
- threats to equipment that is not protected by physical measures (typically smart locks, cameras...).

These are also related to attackers with very high skills and motivation profiles (which is for example the model used in smartcards). In the Smart Home context, this could typically apply to Advanced Persistent Threats (APT) or surveillance topics, where the physical tampering of Smart TVs could turn them into unwanted surveillance tools. This study aims at defining a minimum baseline of security, thus will not address these "high profile" attacks. For information, the security hardware that can be used in several Smart Home devices (smartcards, TPMs) typically include countermeasures against this type of attacks, for example:

- Use of tamper-resistant hardware such as Active shields.
- Protection against glitch.
- Protection against fault injection.
- Protection against side channels (for example electromagnetic or power analysis).

- **Software self-protection:** software also contributes to protect existing security functions, typically by validating inputs and outputs, or by separating the capacities of the different software components (levels of trust, virtualization...).
- **Non-user data protection:** data used to enforce the security functions should be protected. These measures intend to avoid storing internal keys as cleartext, or any other data that could be used to circumvent the service security.
- **Hardening:** hardening consists in reducing the attack surface of the product or device. This includes removing unused services or interfaces (for instance remote shell access to the device, which should not be needed in production),¹⁰⁷ as well as integrating malware protection.

Most of the self-protection measures must be considered from the early design phases. Only the hardening can be defined as an additional measure that can take place after the design and implementation phases.

Implement tamper evidence / tamper resistance for hardware self-protection

Applies to remote services, high-capacity devices

Devices vendors should be aware of the following mechanisms in order to limit hardware and/or software tampering of their devices and services:

- Basic to moderate “tamper resistance” mechanisms, which will slow an attacker (this typically includes specific sealing methods for the casing, or the use of epoxy to protect components, or the entire board, disconnection of debug ports, integration of a Trusted Platform Module...).
- Basic to moderate “tamper evidence” mechanisms, such as tamper-evident seals or labels, or even switches or sensors (light, power...) that will trigger a tamper response.
- Basic to moderate “tamper response” mechanisms such as sending an alarm to a remote service, logging a security error or erasing sensitive data.

While they may not be recommended for every case, vendors should consider using them depending on the level of sensitivity of the assets stored on the device, or the intrinsic value of the device itself. In particular, even constrained devices could be able to implement some kind of tamper evidence, even if they are not able to implement resistance and response.

More details on anti-tamper technologies can be found at different sources, for example Black Hat¹⁰⁸ or ICCV¹⁰⁹ conferences.

Implement hardware self-protections at the design level

Applies to remote services, high-capacity devices

Hardware design can be used to make the device harder to attack. In particular:

- Memory (including memory controller) can include measures such as:
 - Secure erase and wear levelling.
 - Direct memory access, Non executable memory, ...

Examples can be found for example in Security of Things: An Implementers’ Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group. Even if this level of security cannot be required for all Smart Home devices, several physical protection measures can be recommended to ensure a better overall security on the device.

¹⁰⁷ Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities, Rapid 7, September 2015

¹⁰⁸ Introduction to Embedded Security, Joe Grand, Black Hat USA 2004

¹⁰⁹ Physical protection: Anti-tamper mechanisms in Common Criteria security evaluations, Epoche & Espri, ICCV Norway 2010

- Printed Circuit Board (PCB) design can contribute to security by including:
 - Blind and buried vias.
 - Buried bus lines.
 - Electronic fuses and similar techniques, for example to deactivate JTAG access (other uses can also be considered).
- System on Chip (SoC) design can include some of the previous measures, and can also include:
 - Pin placement.¹¹⁰
 - The implementation of “system level” features such as HW Virtualization, micro kernels, Secure boot, Trusted Execution Environments...¹¹¹

The ease of access to the components, as well as their removability, can also be considered during the design phases, even if it cannot be the primary physical protection measure.

Protect the software security functions with self-protection measures by reinforcing interfaces and strengthening the application separation at runtime

Applies to remote services, class 1 devices and higher

Software can contribute to self-protection measures for instance for robustness of interfaces against bad inputs.¹¹² Secure implementation, thoroughly tested, will protect against common attack vectors such as:

- Buffer/heap overflows.
- OWASP’s List of the Top Ten Web Vulnerabilities:¹¹³
 - Injection flaws.
 - Broken authentication.
 - Cross-site scripting (XSS).
 - Insecure direct object references.
 - Security misconfiguration.
 - Sensitive data exposure.
 - Missing function-level access control.
 - Cross-site request forgery (CSRF).
 - Use of components with known vulnerabilities.
 - Invalidated redirects and forwards.

This includes robustness of network interfaces against buffer overflows or fuzzing.¹¹⁴

¹¹⁰ “Security of Things: An Implementers’ Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group” states that “For chips with security features or functionality that may impact security it is important to understand where these are located on the chip’s pin out. It is generally advisable not to use chips where these features are on the outer two rows in high-security environments due to risk of fly wires being used.” Some labs consider today that for “grid array” chip carriers, the outer three or four rows might be relatively easy to access for an attacker. In any case, a consensus is needed amongst stakeholders and security labs on this topic, so cybersecurity agencies could provide vendors with clear recommendations.

¹¹¹ See for example IoT-A - D4.2 - Concepts and Solutions for Privacy and Security in the Resilient Infrastructure or <https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf>

¹¹² See Symantec Insecurity in the Internet of things, March 12, 2015

¹¹³ https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

¹¹⁴ OWASP I3 | Insecure Network Services

Implement trust zones for the execution of applications (and/or ensuring segregation or execution protection), for example by whitelisting applications, or by using Trusted Execution Environments or Secure boot, or SW virtualization...¹¹⁵

Provide a secure default configuration

Applies to remote services, class 1 devices and higher

The default configuration of devices and services should be secured.

The operation mode of the device (or service) should be the most secure one by default. A user might arguably want to disable a given security function, but this should be the consequence of a deliberate action from the user, and the user should be warned that this change reduces the security of the solution.

Providing a secure configuration by default means in practice that:

- A remote service will use HTTPS by default.
- Setup wizard for devices should include the necessary steps to upload any security configuration data such as certificates.
- Stronger password policies will be selected by default...

Provide protection measures for security-enforcing data

Applies to remote services, class 1 devices and higher

Encrypted storage is not only useful to protect user data, but also to protect data that is needed to enforce security on the device.¹¹⁶

Internal data may be just as sensitive as user data, but are often not protected enough, leading for example, to situations where “hardcoded root credentials, API keys for Amazon Web Services, URLs never meant to be known to end-users, and manufacturing network configurations”¹¹⁷ can be found in cleartext on devices.

As a general rule, configuration data should be encrypted at rest and in transit.¹¹⁸

Perform hardening on both HW and SW

Applies to remote services, class 1 devices and higher

Perform hardening to reduce the attack surface: remove unused services or interfaces, integrate dedicated security software, activate memory or control flow protections.

For devices that have a complete operating system, several measures can be considered to harden the device, such as ASLR, non-executable memory, process segregation or sandboxing.

¹¹⁵ See for example Symantec Insecurity in the Internet of things, March 12, 2015, IoT-A - D4.2 - Concepts and Solutions for Privacy and Security in the Resolution Infrastructure or <https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf>

¹¹⁶ See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right and OWASP I10 | Poor Physical Security

¹¹⁷ See A Primer on IoT Security Research, March 30 2015, Stanislav

¹¹⁸ See OWASP I8 | Insufficient Security Configurability and See Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group

Another measure is removing unused tools, services and libraries.¹¹⁹ Unnecessary services should not be present on the device (typically telnet must always be deactivated, but even SSH or FTP can be deactivated in many cases). This type of measures is also applicable at a network level: the device should not leave open ports, especially ports that could be exposed via plug-and-play protocols.¹²⁰

The default configuration of the device should be based upon the most secure parameters, and users should be warned if they have the possibility to roll back to less secure parameters. For example multi-factor authentication should be the default configuration. Users should be warned if they want to configure the service to single-factor authentication.

Vendors should also consider integrating malware protection to their systems¹²¹ since the Smart Home ecosystem provides many possible ways for malware to enter a device (mobile, personal computer, device network interfaces...).

Eventually, vendors should consider deactivation or protection of the external interfaces¹²² for example:

- Protecting the physical debug interfaces such as JTAG/ISP (by password and physical action), or physically deactivate the physical debug access.
- Including mitigation to avoid exploitation of interfaces such as I2C/SPI buses or serial interfaces.
- Suppressing the administration interfaces or limiting it to a local access.¹²³

More generally, vendors should consider their means of protection for:

- BootROM interface.
- Firmware update interfaces.
- Configuration and calibration interfaces.
- Inter-processor IPC.
- USB external interfaces.
- Protection against DMA attacks.¹²⁴
- No unnecessary external interfaces should be accessible from the exterior of the device.¹²⁵

¹¹⁹ See Symantec Insecurity in the Internet of things, March 12, 2015 and The Internet of Fails Where IoT Has Gone Wrong and How We're Making It Right

¹²⁰ See Home Automation Benchmarking by SYNACK, or OWASP I3 | Insecure Network Services

¹²¹ See Symantec Insecurity in the Internet of things, March 12, 2015

¹²² See for example Veracode White Paper – The Internet of Things: Security Research Study or Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group

¹²³ see OWASP I10 | Poor Physical Security

¹²⁴ https://en.wikipedia.org/wiki/DMA_attack

¹²⁵ see e.g. OWASP I10 | Poor Physical Security

6. Good practices for the integration of devices in the Home Area Network

Security of the devices and services is not sufficient in a dynamically connected environment. The Smart Home device is usually connected to a controlled network, typically the Home Area Network. This network can bring additional security features. We suggest to introduce “resilience” as “the network capacity to ensure security control over the devices it contains.”

As examples of such features, a HAN smart hub or gateway can provide resilience on the HAN by providing firewalling, authentication, or malware detection. In the same manner, a mobile network operator can provide resilience on the mobile network by providing authentication, encryption, or anti-spam.

This study distinguishes between three main categories of good practices related to this topic:

- Devices in the HAN should provide minimum *reliability*, even if they are not completely *secured*.
- There should be a mean to give *trust levels* to devices connected the HAN.
- Additional network security measures should be provided on the HAN, for example by dedicated Smart Home gateways, ISPs set-top-boxes, or via service providers (such as anti-virus or firewall specialists).

6.1 Minimum reliability

Hardware must provide basic reliability measures to resist outages and jamming

Applies to class 0 devices and higher

The typical examples are:

- In case of outage (power, network or simply the associated cloud services):
 - Provide the user with a notification¹²⁶
 - Provide smart fail-safe mechanism or standalone option¹²⁷ (if an outage or denial of service happens, devices should be able to go offline, continue to provide their functionalities, and synchronize to remote services as soon as they become available again).
- For network: use the diversity of available interfaces (including hardwired connections) or RF spectrum to maintain connection.¹²⁸
- For power: use battery back-up and/or alternate charging options.

These methods are not exclusive and should all be regarded as good practices. Be careful however when providing interface redundancy, since it increases attack surface. Therefore, more interfaces will have to undergo a security assessment (see [good practices on self-protection](#)).

The hardware itself should be as reliable as possible. The strict requirements of safety-critical hardware cannot possibly apply to Smart Home, but it should be noted that even consumer-grade equipment comes with an estimation of the Mean Time Between Failures (MTBF) or the Annual Failure Rate (AFR).¹²⁹ Be able

¹²⁶ see Symantec Insecurity in the Internet of things, March 12, 2015

¹²⁷ see Symantec Insecurity in the Internet of things, March 12, 2015

¹²⁸ See Home Automation Benchmarking by SYNACK

¹²⁹ See for example http://knowledge.seagate.com/articles/en_US/FAQ/174791en?language=en_US

to monitor and/or advertise these notions should also be considered a good practice for reliability or availability.

In terms of security, the benefits of these availability and reliability measures are twofold:

- It provides a basis for robustness against jamming and denial of service attacks.
- It gives confidence in security alerts: if a device does not behave correctly, it should be an indication of an attack, and not an accident. This is typically a requirement so that additional security controls can be performed on top of the device.

Software components of the Smart Home must handle data changes without failure, errors and improper functioning

Applies to class 0 devices and higher

Software reliability is more difficult to define and assess. This leads to assurance quality measures for which many standards and practices exist. While such measures could make sense in safety-critical software, the cost-to-benefit must be carefully balanced. These issues are out of scope of this study, which focuses on more basic good practices:

- The usage of standard frameworks or communication protocols.¹³⁰
- The notification of users in case of errors, updates or possible compromising.¹³¹
- The implementation of event logging and security audit with forensic enablement in mind.¹³²

6.2 Trust relationships

Use a trust infrastructure within and outside the HAN

Applies to remote services, class 1 devices and higher

Using a trust infrastructure give assurance in heterogeneous environments where devices may enter or quit a given networks, and cannot necessarily be trusted by default.¹³³ Smart Home is a good example of environments where trust is needed:

- between the devices; and
- between the devices and remote services.

The former may be managed locally by a gateway, while the latter could be answered by dependable solutions such as:

- A Public Key Infrastructure.
- Mutual authentication schemes based on shared secrets.¹³⁴
- Alternative schemes such as Identity-Based Cryptography (IBC) and Identity-Based Encryption (IBE).

¹³⁰ See for example See Home Automation Benchmarking by SYNACK

¹³¹ See for example *The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right*, or OWASP I8 | *Insufficient Security Configurability*

¹³² See for example *Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond*, NCC group, or OWASP I8 | *Insufficient Security Configurability*

¹³³ See for example IoT-A - D4.2 - Concepts and Solutions for Privacy and Security in the Resolution Infrastructure

¹³⁴ For example, the Thread group uses J-PAKE, see Thread commissioning, July 2015,

http://threadgroup.org/Portals/0/documents/whitepapers/Thread%20Commissioning%20white%20paper_v2_public.pdf

All these solutions have limitations and vulnerabilities, and should be implemented with these issues in mind.

The following are some examples of key limitations and vulnerabilities:

- A PKI may be complex to administer and maintain, especially when used by a fleet of heterogeneous devices. Revocation mechanisms and multiplicity of authorities add complexity to the infrastructure. Since several possibilities exist, manufacturers and service providers need to understand the security implications of operating a PKI either directly or via a third-party provider.
- Some devices in Smart Home use cases may not be able, for performance reasons, to perform public key cryptography, which is required for most all these schemes. Even a scheme based on pre-shared secrets might use public-key cryptography, for example to enable the renewal of pre-shared secrets, or their revocation if they have been compromised.
- A trust infrastructure is notoriously easy to be implemented wrong, especially for non-specialists. This could lead to vulnerabilities in many devices, giving a false sense of security to their users. For example, even with a complex PKI, vendors are sometimes forced to define additional security measures such as certificate pinning or the use of pre-shared keys.
- History shows that the lack of a proper user interface emphasizes PKI-related vulnerabilities.^{135 136}
- Amongst alternative schemes, IBE/IBC schemes were the subject of several research activities in the recent years and claim a much simpler infrastructure than PKI. The *practical* gap between IBE/IBC and PKI, however, might be smaller than advertised. Eventually IBE might also come with equivalent limitations or vulnerabilities.¹³⁷ We did not find evidences of applications of such schemes in Smart Home. However, some research projects are applying it to smart grids.¹³⁸

The variety of means to establish trust has already been studied by many industry actors, and existing good practices could be used by Smart Home.¹³⁹

Using a trust infrastructure requires skills. Vendors without previous security experience are advised to get third-party support.

Use secure pairing for devices

Applies to remote services, class 1 devices and higher

A strength of Smart Home, when compared to other IoT use cases, is the fact that the end user has a physical access to all the devices. For this reason, secure pairing¹⁴⁰ should also be considered as an additional measure to enforce trust relationships.

¹³⁵ See Fact sheet FS 2011-07 DigiNotar certificates and machine-to-machine (M2M) communication, GOVCERT.NL

¹³⁶ See <http://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html>

¹³⁷ See *A comparison between traditional Public Key Infrastructures and Identity-Based Cryptography*, Kenneth G. Paterson and Geraint Price and *Identity-based cryptography: Panacea or Pandemonium?* Kenny Paterson, ECC 2005

¹³⁸ See <http://scissor-project.com> and related paper at <http://www.wseas.us/e-library/conferences/2015/Dubai/CEA/CEA-01.pdf>

¹³⁹ See for example OneM2M TS-0003-V1.0.1, Security solutions, 30 January 2015

¹⁴⁰ An overview of the different methods, albeit not focused on security, can be found in *A comparative study of secure device pairing methods* (ArunKumar, Nitesh Saxena, Gene Tsudik, Ersin Uzun) and *Serial Hook-ups: A Comparative Usability Study of Secure Device Pairing Methods* (Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, Yang Wang)

For example in Wi-Fi networks, WPS pairing can be securely achieved by a physical action (*WPS one-button-connect*) while the PIN-based WPS is vulnerable to brute-force attacks.¹⁴¹

Check the security assumptions at installation time

Applies to remote services, class 1 devices and higher

The devices and services made assumptions to ensure that the security requirements are sufficient.

Users should be encouraged to check at installation time whether these assumptions are valid as well as the limitations in the usage of the device. For example, a devices using ZigBee connectivity to transmit security alarms might not be able to communicate properly when deployed behind a very thick wall.

Users should be invited to check that the installation conditions in their home allows the operation of all security functions.

6.3 Network security

A gateway can participate in securing Smart Home Environments from internal and external attacks at network level.

Introduce a gateway to mitigate the propagation of attacks from or to the HAN

Applies to remote services, class 1 devices and higher

HAN network security is a useful additional measure to device security. It can mitigate some device vulnerabilities,¹⁴² typically to ensure that data leaks on the HAN cannot “leave the HAN”, and symmetrically that internet threats do not enter the HAN.

Similar functions exist in house devices today. This approach is a logical evolution of these functions:

- The strong protection of the home Wi-Fi network is an example,¹⁴³ provided vulnerable functions such as PIN-based WPS¹⁴⁴ are not used.
- Additional network protection, such as firewall Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) capacities may be available from ISPs, device vendors or other actors (for example in SaaS service such as PC antiviruses). Collecting these data at a central point (*e.g.* in the gateway) enables network operators to detect certain attack scenarios remotely.

This solution leverages on the fact that the HAN contains high-capacity devices that “can be exploited to boost up the security of low-capacity devices by running on their behalf energy-hungry and complex security mechanisms.”¹⁴⁵

These device could notably be able to act as trust systems or facility, particularly for energy-hungry and complex functions such as key management.¹⁴⁶

¹⁴¹ See Stefan Viehböck - Brute forcing Wi-Fi Protected Setup - When poor design meets poor implementation

¹⁴² An Experimental Study of Security and Privacy Risks with Emerging Household Appliances (Position Paper)

¹⁴³ See for example See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

¹⁴⁴ See Stefan Viehböck - Brute forcing Wi-Fi Protected Setup - When poor design meets poor implementation

¹⁴⁵ See for example IoT-A - D1.5 - Final architectural reference model for the IoT v3.0

¹⁴⁶ See for example IoT-A - D4.2 - Concepts and Solutions for Privacy and Security in the Resolution Infrastructure

Network segregation as additional security measure

Applies to remote services, class 1 devices and higher

Network segregation can ensure security for devices and services that have no reason to interact with each other. For that purpose:

- Constrained devices, such as sensors, should not have direct communication outside the HAN. They could rely on the Smart Home gateway or even the ISP's set-top-box to manage long-range connections. This is particularly true for Class 0 devices that have no capacity to manage their own security.
- The same logic can be applied between local networks. If devices can use a HAN which is different from the home Wi-Fi, there is a possibility for the HAN gateway to act as a firewall more efficiently. The use of VLAN might also be considered to segregate traffic type.
- Wireless connections to the HAN should be performed by secure pairing.

Beware that segregation of networks is not a silver bullet: even a Bluetooth interface can be accessed from a relatively long-range with an adequate antenna. For this reason, these network protection measures are only additional measures over device protection functions.

7. Good practices for the usage until end-of-life

This section describes the good practices related to the device once it has been installed by the end-user until its disposal. These good practices consist in three different sets:

- Security good practices for the **protection of data exchanges** with networks accessible to the device.
- **Operation and maintenance** of the security of the device with regards to new vulnerabilities and during device management.
- **Control of user data** on the device.

7.1 Protection of data exchanges

The Smart Home device may be interconnected with several networks. In case of an attack on the device or programming error impacting the network, some separation rules must be followed in order to limit the propagation to other networks.

Ensure access rights

Applies to remote services, class 0 devices and higher

Users shall verify the authorisations given to devices and services for data access and data exchange. This is particularly true in case of an update where access rights may be modified without user's consent.

For example, devices and services can display a comprehensive view of their communications with external devices and services, their requirement to use private data, etc.

Leverage on gateways to reduce the network exposure of the weaker devices

Applies to class 0 devices and higher

Local networks should be separated whenever possible. Each of these networks should be protected by a dedicated gateway (either because they consist of two different networks, or because they consist of two different VLANs managed by a gateway). For example:

- The home Wi-Fi network will be protected by the ISP set top box. This network might include for example entertainment equipment or NAS devices.
- The Home Area Network will be protected by the Smart Home hub or gateway.
- The users might create ad-hoc networks dedicated to some devices. For example a Bluetooth network can include smart lightbulbs and smart locks on the one side and smartphones or tablets, which have access to mobile network, on the other side. To prevent attacks from the smartphones or tablets to the ad-hoc network, users should be encouraged to secure their smartphones and tablets, typically by securely configuring them (password, official application stores only) and using dedicated security applications (anti-virus, protection suites).

Smart Home devices in each of these networks have no reason to access devices in the other networks. Even if it were the case, access should be managed by the dedicated gateways.

Most of Smart Home devices in these networks have also no reason to access the WAN directly, especially since the home is very likely to be connected to an ISP. For this reason, devices should access the WAN only through their dedicated hubs or gateways. This is a significant difference between Smart Home and other IoT contexts, where sensors can be expected to have a direct LPWAN access.

The Smart Home gateways or hubs must implement network protection measures, as described in [Section 6](#).

Some Smart Home devices have a direct access to WAN or LPWAN, for example alarms and surveillance cameras. In this case, the WAN or LPWAN access should not be used to enter the HAN. For this reason, these devices should access local network only through a secure gateway or hub.

Segregate the Smart Home Networks and the AMI

Applies to class 0 devices and higher

Comply with the requirements and recommendations of the AMI gateway if a Smart Meter is installed.

While the security functions of the smart meters or smart energy gateways are out of the scope of this study, in some architectures¹⁴⁷ the gateway to the Advanced Metering Infrastructure is used as an interface to the Home Area Network. To ensure correct operation of the AMI, Smart Home vendors should:

- implement the protection required by the smart gateway, if any; and
- prevent disruption of service, for example causing denial of service by using too much bandwidth.

7.2 Operational security and maintenance

Following the good practices described so far shall significantly reduce the risk of having vulnerabilities found in the product, however this risk can never be avoided. Vendors shall not only pro-actively perform a survey for new vulnerability but also provide a secure and reliable device update mechanism to allow fixing vulnerabilities.

7.2.1 Vulnerability survey

Perform vulnerability survey

Applies to remote services, class 0 devices and higher

Once a device is on the market, the vendor must perform a vulnerability survey and fix security flaws accordingly. The vulnerability survey should include developer findings, on-line researches, CERTs advisories, as well as input from customers¹⁴⁸ and security researches. The end-user must be informed of the support period of the device and of the end of support for security fixes.

A policy for vulnerability handling and disclosure awareness should be defined.¹⁴⁹ Bug bounty programs can also provide an incentive to third-party researchers.^{150 151}

¹⁴⁷ See for example in the BSI Smart Meter Gateway PP: “The Gateway connects a Wide Area Network (WAN) with a Network of Devices of one or more Smart Metering devices (Local Metrological Network, LMN) and the consumer Home Area Network (HAN), which hosts Controllable Local Systems (CLS)”
(https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf)

¹⁴⁸ See The Current State Of Smart Locks

¹⁴⁹ See The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

¹⁵⁰ See FTC Careful Connections

¹⁵¹ See also the global bounty aggregator <https://firebounty.com>

Known vulnerabilities must be patched.¹⁵² A patch may consist of a workaround if the developer did not yet provide a fix. When over-the-air updates are not available, a plan for product recalls shall be considered, so that vendors can implement the patch in the devices.¹⁵³

For online services supporting Smart Home devices, a rollback to a secure state must be possible.

Eventually, vulnerabilities impacting user data should be communicated as transparently as possible. The EU Opinion 03/2014 on Personal Data Breach Notification from the Article 29 Working Party gives examples of such situations.¹⁵⁴

Check the security assumptions regularly during life-time

Applies to remote services, class 0 devices and higher

The devices and services made assumptions to ensure that the security requirements are sufficient. Vendors and users should be encouraged to check regularly that these assumptions are still valid. For example:

- Limitations in the usage of the device (for example, a given device might need ZigBee connectivity to transmit security alarms, implying that it will not be able to send alarms when deployed behind a very thick wall). Vendors could discover that, in the field, the signal requires even stricter conditions (even thinner walls, no interference...). They will need to send users an information so they can check if their installation is secure.
- Assumed properties of the environment (for example, assuming that the certification authorities in the certificate store are all trusted and not compromised). Vendors should perform a survey to be able to remove a compromised CA from the certificate store.
- Assumed properties of cryptographic properties (for example, assuming that a given algorithm and key size are sufficient for a given task). Vendors will need to check regularly this assumption, for example if a new cryptographic attack puts users at risk unless they use longer keys or change their cryptographic suites.

7.2.2 Security updates

Protect the software update mechanism

Applies to class 1 devices and higher

Security updates provide protection against vulnerabilities found during the life of a device or application.¹⁵⁵ However this comes at a cost, since support of this functionality also provides an entry point for an attacker. In particular vendors should:

- Provide automatic and timely security updates.¹⁵⁶
- Protect the updates (typically via encryption and digital signature). The update files must not contain sensitive data.¹⁵⁷ The signature must be verified before the update is applied.

¹⁵² see Symantec Insecurity in the Internet of things, March 12, 2015 or FTC - Careful Connections

¹⁵³ See for example Nest product recall: <http://www.cpsc.gov/en/Recalls/2014/Nest-Labs-Recalls-to-Repair-Nest-Protect-Smoke-CO-Alarms/>

¹⁵⁴ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

¹⁵⁵ see Symantec Insecurity in the Internet of things, March 12, 2015 and Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond, NCC group

¹⁵⁶ see Symantec Insecurity in the Internet of things, March 12, 2015 and OWASP I9 | Insecure Software/Firmware

¹⁵⁷ See OWASP I9 | Insecure Software/Firmware

- Protect the *application of an update* on the device. An attacker should not be able to trigger a firmware installation without an authorization.
- Protect the security update interface against attacks.

7.2.3 Remote interfaces protection

Provide user-friendly interfaces for device and services security management

Applies to remote services, class 1 devices and higher

The ease of use of the user interface must contribute to help users perform correct administrative tasks.¹⁵⁸ Such interfaces can be found for example on the device itself, on a web portal or through a mobile application.

User-friendliness helps maintaining a secure state on the device by:

- Giving more chance that simple actions such as firmware update or password changes are effectively performed by the user.
- Providing an accurate description of the security status of the service, and explaining what actions can contribute to mitigate potential threats.

Vendors and service providers should also raise their users' awareness about infected e-mails and hoaxes.

Protect remote monitoring interfaces

Applies to remote services, class 1 devices and higher

Protection of remote monitoring interfaces is crucial since they often provide a highly-privileged entry point into a device. This protection includes access control and authentication mechanisms, as described in good practices on Identification, authentication, authorisation.

7.2.4 Security management system for support infrastructures

Rely on existing sources for security good practices in order to secure infrastructures

Applies to remote services, class 1 devices and higher

Regarding the requirements for remote infrastructures related to Smart Home, there is no specific needs in the Smart Home use case compared to usual cloud services or usual device support infrastructures.

For this reason, the main recommendations would consist of:

- *Security management*: As a general rule, implement an information security management system (ISMS) as described in the ISO 27001. ENISA recommendations apply.¹⁵⁹
- *Secure development*: as a general rule, follow the recommendations issued by OWASP, especially (but not limited to) the following:
 - Top 10 project.
 - Testing project.
 - Web Testing Environment Project.
 - Application Security Verification Standard Project.
 - Software Assurance Maturity Model.
- *Security assessment*: we recommend that service operators:
 - Ask for third-party audits on their infrastructures (such audits may be part of an ISO 27001 certification).

¹⁵⁸ See What to Consider When Buying a Smart Device, TrendMicro

¹⁵⁹ See ENISA - Auditing Security Measures - An Overview of schemes for auditing security measures, September 2013

- Ask for third-party penetration testing of their services, including at least a network scan and if possible, manual penetration testing.

Regarding Cloud computing, service providers should consider certification following ENISA recommendations.¹⁶⁰

7.3 Control of user data

Provide secure backup and/or deletion of the data stored/processed by the device (and by associated cloud services) during the operation and at end-of-life

Applies to remote services, class 1 devices and higher

The end-user must have a way to securely erase its private data collected by or stored on a Smart Home device.

More generally, a secure factory-reset of the firmware and configuration should be available on the device.

For client information in remote infrastructures such as cloud services, data sanitization must be in place.¹⁶¹

For user data present on devices, secure deletion of encryption keys may provide enough protection, assuming that data is encrypted in conditions that guarantee long-term confidentiality (see [good practices on Cryptography](#)).

Metadata should be erased the same way as other sensitive data, since the same threat apply (see [good practices on User data protection](#)).

¹⁶⁰ See <https://resilience.enisa.europa.eu/cloud-computing-certification>

¹⁶¹ Description of typical measures and issues can be found in NIST *Guidelines on Security and Privacy in Public Cloud Computing*

8. Recommendations

8.1 All stakeholders should reach a consensus on minimum security requirements

This recommendation is mainly intended for vendors and service providers, national cybersecurity agencies, consumer groups, standardisation bodies and/or industry associations

This study identified several groups of good practices related to Smart Home Environments. For some of these topics, dedicated security standards or initiatives already exist.¹⁶²

It is important that all stakeholders involved reach a consensus on good practices in order to build a widely accepted set of requirements for Smart Home. By relying on *national cybersecurity agencies* and *consumer groups* on the one hand, and *standard groups* and *industry associations* on the other hand, the Industry can converge toward a unique set of minimum security requirements.

These minimum security requirements should target the whole ecosystem of a Smart Home: interconnected devices, services and networks. They could be tailored for IoT or specifically for Smart Home Environments and should target specific IoT security concerns, beyond the usual security requirements (for example related to web security).

The objective of this recommendation is also to clarify which Smart Home specific strengths can be leveraged upon to provide efficient security functions, in particular for devices related to health and safety and devices with low capacity (class 0 and class 1).

A consensus can also be a first step for industry associations and standards groups to build compliance tools, such as a testing guides.¹⁶³ Industry associations and standard groups could therefore define requirements with compliance testing in mind.

8.2 Industry actors should support security-driven business models

This recommendation is mainly intended for vendors, policy makers, industry groups and consumer associations

Smart Home, at least in its consumer-market part, is mainly cost-driven. As a consequence, functionalities usually has priority over security for both vendors and end-users. This leads to an increase of vulnerabilities, with increased security concerns that can have an impact on the Home and its inhabitants as it happened recently in the automotive domain.¹⁶⁴

It is recommended that security becomes a requirement for all products and services that have an impact on user's life and safety.

For that purpose, vendors and policy makers should understand their users' expectations of safety, security and privacy. They should propose a secure version of their products or even integrate security in their product *by default*.

¹⁶² See for example <http://www.homegatewayinitiative.org/>

¹⁶³ See for example OWASP testing guide

(https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)

¹⁶⁴ See <http://arstechnica.com/security/2015/08/uber-hires-researchers-who-hacked-chrysler-uconnect/>

Consumer associations should raise the issue and discuss with industry groups to provide requirements on “secure options”, and how “secure” and “non-secure” options should be advertised so as to provide a fair information to the consumer. An incentive could be to assess the costs of security against the costs of liabilities of an insecure product.

8.3 All actors should contribute to raise security awareness

This recommendation is mainly intended for vendors, consumer associations and national cybersecurity agencies

Security awareness is especially needed since end-users integrate devices and services to control their Smart Home, with a potential impact on their life and safety.

Vendors' awareness

IoT vendors shall keep track of vulnerabilities in other IoT products, especially in the context of Smart Home Environments. For that purpose, vendors can hire or train security experts to understand security vulnerabilities in IoT, as they can only get worse with a wider adoption of the products. It is also important to consider early warnings on security issues provided by users and researchers, as they contribute to reducing the attack surface on devices and services.

By raising the awareness level of IoT companies to security, product security will be improved and vendors will reduce the threats they face and associated reputation issues. It is particularly true for vendors with limited experience in security.

Users' awareness

Users have a *de facto* responsibility on the security of their devices and services connected local networks, yet they may not be aware of that fact. Consumer associations and/or cybersecurity agencies can raise user awareness by providing user support and guidance on several topics such as:

- How to choose a Smart Home device
- How to operate a Smart Home device
- How to control online services etc.

Vendors should also contribute to this awareness by explaining clearly how to properly configure their devices, the security properties available and the consequences of an insecure configuration.

In this context, vendors as well as consumer associations might contribute to establish user guidance (see for example [Annex D: Example of topics for user awareness](#)).

8.4 Industry actors should develop security assessment methods or frameworks

This recommendation is intended for industry associations, the European Commission and its Member States, national cybersecurity agencies, standardisation bodies

The security of IoT in Smart Home Environments depends on several constraints not covered by existing security assessment methods or framework. It is important to understand how Smart Home devices, regardless of the regulation, will not be able to resist cyber-attacks which can originate from inside or outside the Home.

For that purpose, industry associations, the European Commission and its Member States (for example through their national privacy agencies) should define rules to ensure the level of security of a given product. Such security assessment method could be targeted at manufacturers, vendors and/or end-users.

It is recommended that such security assessment method combines and adapts existing work such as:

- Whitelisting or certification of vendors.
- Integration of multiple levels of assurance to counter attack with different impact
- Defining the rules for security audit and testing (e.g. self-assessment, third party assessment, certification...)

It is also recommended to collaborate with CERTs or external third-party to demonstrate resistance to existing attacks using at minimum well-known/public vulnerabilities assessment as well as black-box vulnerability testing campaign or a code/configuration review.¹⁶⁵ Enhanced security assessment could integrate product-specific vulnerability assessment as well as grey- or white-box vulnerability testing campaign and/or a fuzzing campaign¹⁶⁶.

Note that manufacturers and developers with limited experience in security are strongly encouraged to rely on:

- Security researchers (academics) or private evaluation facilities, that have the skills to perform these tasks.
- National cybersecurity agencies or industry associations, that are able to clarify the expected effort and methods for these tasks.

8.5 Policy Makers should clarify the legal aspects of Smart Home Environments

This recommendation is intended for: policy makers from the European Commission and in its Member States

A compromised Smart Home component could have a severe impact in terms of security, privacy and safety in many cases (smart locks, thermostats, smoke or CO₂ detectors...). Technical measures could address a good part of such risks. However, their adoption might be expensive and there is no clear incentive to naturally regulate vulnerable solution. Hence, it is important to define liabilities through policy.¹⁶⁷

For that purpose, Policy makers should clarify the liability issues related to Smart Homes by defining:

- The liability of industry players in cases of damages or injury, if a compromised device fails to meet its safety goal.
- The liability of industry players whenever a private data breach occurs.

Moreover, the European Commission and Member States should clarify:

- How long companies should be liable for fixing known vulnerabilities.
- The liability of companies not disclosing, and not fixing, potential vulnerabilities.

¹⁶⁵ Code review typically in the case of mobile applications or embedded systems. In the case of more complex systems or even infrastructure, a configuration review would be more appropriate.

¹⁶⁶ White-box consists in testing a product with all the design and development knowledge, including source code. A grey-box approach would consist in not having the code but developer information such as credentials. Fuzzing is a black-box approach (no information is known on the product), where random data is given to the product to assess its robustness. The automation of the method is intended to compensate the lack of knowledge on the product.

¹⁶⁷ See for example Who Should be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments, Terrence August and Tunay I. Tuncay, March 2011

- A legal framework for disclosure of vulnerabilities by academics or private-sector researchers knowing that:
 - Companies should be able to have enough time to fix vulnerabilities before a disclosure is made.
 - On the other hand, a company should not be able to prevent or limit the disclosure of a vulnerability (not being public does not prevent a vulnerability to be found and exploited by several actors). This should be a requirement especially when a company does not provide fixes or workarounds to mitigate the associated threat.

Note that liability could provide an incentive to implement security correctly, as it is already a part of the CE marking process (in case of damages or injuries). Yet, several risks and limitations that should be avoided to limit financial risks, unfair situations to smaller players, and the scope of application.

8.6 Industry research and publicly-funded initiatives should integrate cyber security in R&D projects related to Smart Home and IoT

This recommendation is mainly intended for vendors, academics, and policy makers which fund research

While many good practices are already available for Smart Home vendors to implement security, some of them have limitations or could be improved.

The European Commission and its Member States (MS), research and development competent authorities in cooperation, the Academia and R&D sector should develop incentive to integrate cyber security in existing research programmes, such as FP7 and Horizon 2020.

Moreover, projects managers should:

- Define which part of their project needs to consider cyber security.
- Evaluate security requirements that shall cover identified cyber threats.
- Explain to which extent their project integrates cyber security.

For research and development projects focusing purely on security, current research indicates new mechanisms that could provide additional protection (for example Anonymous signatures¹⁶⁸ or authentication,¹⁶⁹ homomorphic encryption¹⁷⁰ or secure multiparty computation.)¹⁷¹ These project should contribute to securing Smart Home Environments (for example, by defining trust relationships within heterogeneous home networks, by overcoming the issues of class 0 or class 1 constrained devices...)

¹⁶⁸ See <https://abc4trust.eu>

¹⁶⁹ See ISO/IEC 29191, ISO/IEC 20008 and ISO/IEC 20009. This “anonymous authentication” should not be mistaken for the “anonymous authentication” as defined in Microsoft IIS.

¹⁷⁰ See <https://crypto.stanford.edu/craig/craig-thesis.pdf>

¹⁷¹ https://en.wikipedia.org/wiki/Secure_multi-party_computation

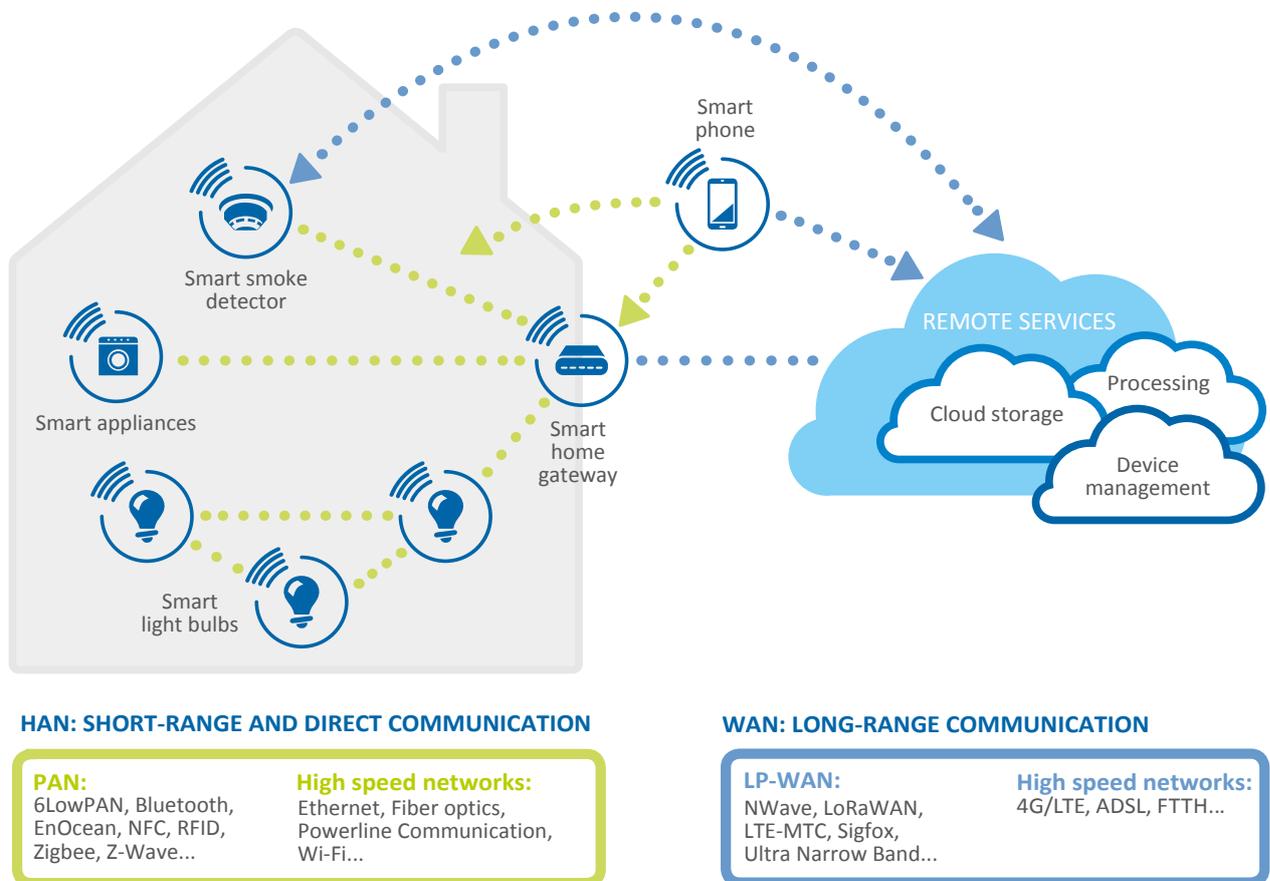
Annex A: Additional details on Smart Home Environments

A.1 Communications

As presented in Figure 4, Smart Home devices include a very high number of communication means:

- Direct or short-range communication is used within the home
- Long-range communication is used to access the remote services associated with the devices, and is also present due to the existing connectivity in the home.

Figure 4: Communications in Smart Home Environments



A.1.1 Technologies

Smart Home devices typically have one or several interfaces to different ranges of communication. They can use direct communications with other devices (that may be Smart Home devices or personal computers, smartphones...), ad-hoc and multi-hop communications.

Short range communication on the Home Area Network

Short range communications include both low speed Personal Area Networks (PAN) using and high speed networks. They can implement wireless or wired connections.

Wireless protocols vary from standards such as 6LowPAN, Zigbee, Bluetooth or Wi-Fi, but also proprietary protocols such as Z-Wave or EnOcean.

Wired connections include Ethernet, Fiber optics, Powerline Communication or telephone wires.

Long range communication over a Wide Area Network:

For long-range communications and Internet connectivity, devices can rely on their own connectivity or use a gateway be it the Smart Home gateway or a smartphone.

WAN communications are possible at low speed through Low-Power Wide-Area Networks (LPWAN), with approaches such as LoRaWAN (often abbreviated into LoRA), Ultra Narrow Band (*e.g.* SigFox) and many others such as LTE-MTC, NWave...

High speed WAN communications may also be available using Internet through a gateway or a set-top-box, a direct 4G/LTE connectivity...

A.1.2 Protocols

On top of these communication technologies, devices implement several higher-level protocols, some of them being dedicated to IoT. For example, the following protocols are used in various contexts:

- Messaging protocols with a many-to-many approach
 - Example: MQTT (adapted into MQTT-SN, for non TCP/IP protocols such as ZigBee).
- Webservice protocols, or document transfer protocols, with a client-server approach
 - Example: HTTP for TCP/IP protocols.
 - Example: CoAP (initially built for UDP protocols).

A.1.3 Security

The usage of dedicated security mechanisms varies depending on the solution used. Several approaches are taken, from the transport to the applicative layer:

- User authentication/authorization protocols such as Oauth / OpenID, XACML/SAML Single sign-on etc.
- Communication protection protocols such as SSL/TLS over TCP/IP, or DTLS over UDP.
- Usage of cryptographic algorithms to secure transport layer is found amongst many of the communication protocols.

A.2 Platforms

A Smart Home platform integrates a set of:

- Hardware.
- Operating System.
- Additional software (*e.g.* communication stacks).
- Related remote services (*e.g.* analytics, device management or provisioning).

While the platform includes all these elements, it has to be noted that in many cases there are different providers for these parts. Typically low cost devices can be built upon cheap Hardware, using one of the many open source OSes available (TinyOS, Contiki, FreeRTOS, Mantis OS, Nano-RK, LiteOS...).

The environment of the platform is:

- The service infrastructures providing the remote services and their applications.
- The networks (both the HAN and the WAN) and the objects attached to it:

- Objects attached to the HAN such as smartphones, tablets or PCs.
- Other Smart Home platforms.
- Other actors, for example web services, accessible through the WAN.

It has to be noted that devices may enable privileged pairings with any of these elements. For example:

- A smart lock can be paired with the user's smartphone.
- A smart hub is intended to be paired with the other Smart Home devices.
- A smart TV can be paired with third-party cloud services such as entertainment providers, or social networks.

Annex B: Mapping threats with good practices

The threats of the ENISA threat landscape are mapped to good practices in Table 2 in order to highlight specific countermeasures. The good practices are associated to the lifecycle of devices and services in Smart Home Environments.

Some threats were merged for readability reasons, and some threats were not mapped to good practices: this does not mean that the threats are not applicable to the Smart Home use cases, but only that these threats will have to be considered *after a first set of good practices are already in place*.

The Several good practices are generally not included in the table, because they are implicitly used by most of the security functions. These good practices are:

- Logs and audit measures must cover, and contribute to, all the security functions.
- Cryptography is the basis of most security functions.
- User should be notified whenever security is at risk.

However, in some cases they are included in the mapping hereafter, mostly when they are considered as the main security countermeasure to a given threat.

Table 2: Mapping threats with good practices

THREAT	GOOD PRACTICES	RATIONALE
Legal		
Not addressed in this study except for select privacy issues. See good practices for the Development phase on User data protection .		
Nefarious Activity/Abuse		
Identity fraud	Development <ul style="list-style-type: none"> • Identification, authentication, authorisation • User data protection Usage until End-of-Life <ul style="list-style-type: none"> • Operational security and maintenance (Section 7.2) 	Identity fraud must be addressed not only by credential protection, but also by the protection of private data that might contribute to impersonation. Consequently this is also covered by privacy measures.
Unsolicited & infected e-mail Hoax	Development <ul style="list-style-type: none"> • Self-protection • Communication protection 	This topic can typically be addressed by awareness campaigns from the vendors and service providers.

THREAT	GOOD PRACTICES	RATIONALE
<p>Unsolicited & infected e-mail</p> <p>Hoax</p>	<p>Integration</p> <ul style="list-style-type: none"> • Good practices for the integration of devices in the Home Area Network (Section 6) <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> • Operational security and maintenance (Section 7.2) 	<p>This topic can typically be addressed by awareness campaigns from the vendors and service providers.</p>
<p>Denial of service</p>	<p>Development</p> <ul style="list-style-type: none"> • Communication protection <p>Integration</p> <ul style="list-style-type: none"> • Good practices for the integration of devices in the Home Area Network (Section 6) <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> • Operational security and maintenance (Section 7.2) 	<p>Failsafe mechanisms, multiplicity of interfaces and user notification should ensure a minimum level of robustness against denial of service. The protection of communications also addresses these concerns.</p>
<p>Malicious code/software activity</p>	<p>Development</p> <ul style="list-style-type: none"> • Self-protection <p>Integration</p> <ul style="list-style-type: none"> • Good practices for the integration of devices in the Home Area Network (Section 6) <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> • Operational security and maintenance (Section 7.2) 	<p>Self-protection must cover the vulnerabilities related to malicious code.</p> <p>Another way to mitigate these threats consists in additional Home Area Network protection and management of trust relationships to isolate compromised devices.</p>
<p>Abuse of information leakage</p>	<p>Development</p> <ul style="list-style-type: none"> • Security of the development process (Section 5.1) • User data protection <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> • Good practices for the usage until end-of-life (Section 7) 	<p>Security administration functions must also be available (Security management). Eventually, the design should lead to understandable and usable user interfaces.</p> <p>Privacy and confidentiality requirements also require transparency, so that the user is aware of the type of data that are potentially at risk.</p>
<p>Generation and use of rogue certificates</p>	<p>Development</p> <ul style="list-style-type: none"> • Identification, authentication, authorisation 	<p>The trust infrastructure must cover the risks of public key vulnerabilities.</p>

THREAT	GOOD PRACTICES	RATIONALE
Generation and use of rogue certificates	Integration <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) 	The trust infrastructure must cover the risks of public key vulnerabilities.
Manipulation of hardware & software	Development <ul style="list-style-type: none"> Security of the development process (Section 5.1) Self-protection 	<p>Development security must ensure that unauthorized manipulations are not possible during production.</p> <p>After delivery to the end-user, the device must be self-protected.</p>
Manipulation of information	Development <ul style="list-style-type: none"> Communication protection Security audit Integration <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) Usage until End-of-Life <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	<p>Trust and reputation relationships, associated to communication protection, must cover the risks of external information manipulations</p> <p>Manipulation of the audit trail must not be possible</p>
Misuse of audit tools Falsification of records	Development <ul style="list-style-type: none"> Security audit User data protection Self-protection 	<p>Audit tools must be protected from unauthorized access. Furthermore, privacy requirements contribute to reduce the amount of potentially exploitable data</p> <p>Self-protection contributes to mitigate the risks of manipulation by malicious code on the device.</p>
Unauthorised access to information system/network Unauthorised use of administration of devices & systems Abuse of authorizations	Development <ul style="list-style-type: none"> Identification, authentication, authorisation Usage until End-of-Life <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	Identification, authentication and authorization are a general requirement for the access to sensitive functions. This is particularly the case for administrative capacities.
Unauthorised use of software	Development <ul style="list-style-type: none"> Self-protection 	Self-protection contributes to mitigate the risks of manipulation by malicious code on the device.

THREAT	GOOD PRACTICES	RATIONALE
<p>Unauthorised installation of software</p> <p>Badware</p>	<p>Usage until End-of-Life</p> <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	<p>Security management also state that firmware installation should be protected to ensure its authenticity and integrity</p>
<p>Compromising confidential information</p> <p>Abuse of personal data</p>	<p>Development</p> <ul style="list-style-type: none"> User data protection 	<p>Private information must be protected from unauthorized access. Furthermore, privacy requirements contribute to reduce the amount of potentially exploitable data</p>
<p>Remote activity (execution)</p>	<p>Development</p> <ul style="list-style-type: none"> Communication protection Identification, authentication, authorisation Self-protection <p>Integration</p> <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	<p>The remote capacities of a device must be available only to authorized users – and they should be performed by secure channels.</p>
<p>Targeted attacks (including APT)</p>	<p>These attacks are not considered here due to the very high potential of the attacker, with regards to the assets. This topic should be addressed by national cybersecurity agencies.</p>	
<p>Eavesdropping / Interception / Hijacking</p>		
<p>War driving</p>	<p>Development</p> <ul style="list-style-type: none"> Communication protection <p>Integration</p> <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	<p>Devices and services must implement secure communications.</p> <p>However there are some devices that lack capacities for this, and in the case of war driving, the attacker aims at the Home Area Network. For this reason, the additional network protection on the HAN is particularly critical with regard to this threat.</p>
<p>Interception compromising emissions</p>	<p>Such side-channel attacks are not considered in this study, since they require a relatively high attack potential.</p> <p>As far as Smart Home is concerned, the stocktaking and the interviews showed that communication protection is still more an exception than a rule, meaning that attackers are more likely to exploit non-protected communications than performing side channel attacks.</p>	

THREAT	GOOD PRACTICES	RATIONALE
Interception of information, Network reconnaissance and information gathering, Replay of messages, Man in the middle/ session hijacking	Development <ul style="list-style-type: none"> • Communication protection Usage until End-of-Life <ul style="list-style-type: none"> • Operational security and maintenance (Section 7.2) 	-
Interfering radiations	Integration <ul style="list-style-type: none"> • Good practices for the integration of devices in the Home Area Network (Section 6) 	Failsafe mechanisms, multiplicity of interfaces and user notification should ensure that interference or jamming do not hamper security
Repudiation of actions	<p>The notion of repudiation comes with the notion of legal or contractual binding. The main use cases foreseen are:</p> <ul style="list-style-type: none"> • Billing (e.g. for protected content in Audio/Visual systems and devices) and • Insurance (e.g. using smart locks or surveillance data). <p>The stocktaking did not show evidences of the latter, while the former belongs in a domain where vendors already have incentives to implement these kinds of security functions. In both cases, the threat would be addressed by digital signature functions in a secure element¹⁷², or by Trusted Platform Modules¹⁷³. For these reasons, the study does not further address these threats.</p>	
Physical attacks		
Simple physical attacks	Development <ul style="list-style-type: none"> • User data protection • Self-protection 	Self-protection includes both physical and logical protections against physical attacks. User data protection also mandates that user data is not easily accessible in cleartext on the device.
Advanced physical attacks	These attacks are not considered here due to the very high potential of the attacker.	

¹⁷² See for example the SSCD Protection Profiles recommended by SOG-IS (http://www.sogisportal.eu/uk/pp_en.html)

¹⁷³ See http://www.trustedcomputinggroup.org/developers/trusted_platform_module

THREAT	GOOD PRACTICES	RATIONALE
Dependability and reliability		
Disasters and outages		
Lack of resources/electricity, Internet outage, Network outage, Strike, Loss of support services	<p>Integration</p> <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	Failsafe mechanisms, multiplicity of interfaces and user notification should ensure that power or network outage do not hamper security
Absence of personnel	<p>Development</p> <ul style="list-style-type: none"> Security of the development process (Section 5.1) 	The design should lead to understandable and usable user interfaces – user guidance also contributes to helping the user making sensible configuration choices
Unintentional damages (accidental)		
Information leakage or sharing Erroneous use or administration of devices and systems	<p>Development</p> <ul style="list-style-type: none"> Security of the development process (Section 5.1) User data protection <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	<p>Security administration functions must also be available (Security management). Eventually, the design should lead to understandable and usable user interfaces.</p> <p>Privacy and confidentiality requirements also require transparency, so that the user is aware of the type of data that are potentially at risk.</p>
Using information from an unreliable source	<p>Integration</p> <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) 	The devices and services must know the level of trust of the information they use.
Unintentional change of data in an information system	<p>Integration</p> <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) 	Components of the Smart Home must handle data changes without failure, errors and improper functioning
Inadequate design and planning or lack of adaption	<p>Development</p> <ul style="list-style-type: none"> Security of the development process (Section 5.1) 	-

THREAT	GOOD PRACTICES	RATIONALE
Damage/Loss (IT Assets)		
Damage caused by a third party	See physical attacks	-
Loss from DRM conflicts	Integration <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) 	Components of the Smart Home must handle data changes without failure, errors and improper functioning. In particular, they should not cause information loss outside of their own perimeter.
Loss of information in the cloud Loss of (integrity of) sensitive information	See “Information leakage” as well as “Eavesdropping / Interception / Hijacking”	
Loss or destruction of devices, storage media and documents	See “physical attacks”, as data leakage from a lost or stolen device is a physical attack	
Information leakage	Development <ul style="list-style-type: none"> User data protection Usage until End-of-Life <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	User data protection includes measures to ensure that these data is not accidentally leaked. User guidance contributes to educate the end-user with that regard
Failures / Malfunctions		
Failures / Malfunctions of parts of devices, Failures / Malfunctions of devices or systems, Failures of hardware, Software bugs	Integration <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) 	Reliability of devices and services is addressed as a basis requirement upon which the security can be built
Failures or disruptions of communication links (communication networks), Failures or disruptions of main supply, Failures or disruptions of the power supply	Integration <ul style="list-style-type: none"> Good practices for the integration of devices in the Home Area Network (Section 6) Usage until End-of-Life <ul style="list-style-type: none"> Operational security and maintenance (Section 7.2) 	Failsafe mechanisms, multiplicity of interfaces and user notification should ensure that power or network outage does not hamper security

THREAT	GOOD PRACTICES	RATIONALE
Failures of disruptions of service providers (supply chain)	This topic is not developed further in the study, since security organisational good practices address only marginally these issues.	-
Configuration errors	<p>Development</p> <ul style="list-style-type: none"> • Security of the development process (Section 5.1) <p>Usage until End-of-Life</p> <ul style="list-style-type: none"> • Operational security and maintenance (Section 7.2) 	The design should lead to understandable and usable user interfaces – user guidance also contributes to helping the user making sensible configuration choices

Annex C: Checklist of good practices

Table 3 proposes a checklist of good practices and their application to remote services and devices classes. Stakeholders can use this table for example in their risk assessment to cross-check which good practices applicable to secure their devices and services.

The application of good practices to devices classes and remote services is denoted by the following icons:

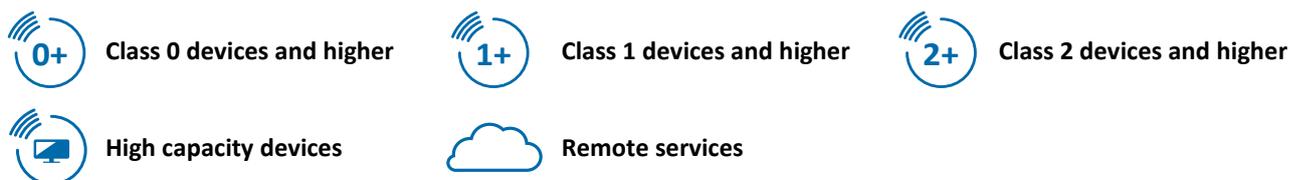


Table 3: Checklist of good practices

GOOD PRACTICES FOR THE DEVELOPMENT OF SMART HOME DEVICES AND SERVICES		APPLIES TO
Security of the development process		
Design phase		
	Use defence in depth	 
	Separate security functions from other functions	 
	Make assumptions for the security requirements explicit	 
	Consider third-party review by security specialists for developers with limited security experience	 
	Prepare user interactions with the products or services	 
Development phase		
	Use configuration management tools, and leverage upon development environments such as compilers or static analysers	 
	Take security into account when choosing your programming language; when available, leverage upon the operating system security functions	 
	Use standard, secure frameworks or stacks whenever possible – do not redevelop security functions	 

Ensure team training and awareness	 
Testing phase	
Test the compliance of security functions	 
Perform additional security audits and penetration testing	 
Perform a privacy assessment	 
Security functions for hardware and software	
Security audit	
Log security events	 
Notifications should be easy to understand and help users find a remediation or workaround	 
Communication protection	
Protect all communication against disclosure, modification and replay	 
Mitigate vulnerabilities or limitations of standard security library	 
Protect communications against denial of service	 
Cryptography	
Do not create proprietary cryptographic schemes, but use state-of-the-art standards instead. Even a home-brewed implementation of a standard is not a good practice when standard implementations are available.	 
Rely on an expert in cryptography for interfacing with HW accelerated cryptography or secure elements, or even using or configuring a standard implementation.	 
When designing or procuring HW, pay attention to the requirements of cryptography in terms of CPU, memory and bandwidth and their impacts on battery.	
Be aware of limitations of HW-based cryptography solutions and choose wisely whether a SW or HW solution is needed for the given context.	

Manage keys securely	 
Use trust and reputation infrastructures	 
User data protection	
Identify personal data	 
Implement transparency measures	 
Design the product/service with legitimate purpose and proportionality in mind	 
Identification, authentication, authorisation	
Use mutual authentication for remote communication	 
Use multi-factor authentication for user authentication	 
Implement access control measures to separate the privileges of different users as well as the privileges of different applications	 
Implement a strong password management policy	 
Enforce session management policies to avoid session hijacking	 
Self-protection	
Implement tamper evidence / tamper resistance for hardware self-protection	
Implement hardware self-protections at the design level	
Protect the software security functions with self-protection measures by reinforcing interfaces and strengthening the application separation at runtime	 
Provide a secure default configuration	 
Provide protection measures for security-enforcing data	 

Perform hardening on both HW and SW	 
Good practices for the integration of devices in the Home Area Network	APPLIES TO
Minimum reliability	
Hardware must provide basic reliability measures to resist outages and jamming	
Software components of the Smart Home must handle data changes without failure, errors and improper functioning	
Trust relationships	
Use a trust infrastructure within and outside the HAN	 
Use secure pairing for devices	 
Check the security assumptions at installation time	 
Network security	
Introduce a gateway to mitigate the propagation of attacks from or to the HAN	 
Network segregation as additional security measure	 
Good practices for the usage until end-of-life	APPLIES TO
Protection of data exchanges	
Ensure access rights	 
Leverage on gateways to reduce the network exposure of the weaker devices	
Segregate the Smart Home Networks and the AMI	

Operational security and maintenance

Vulnerability survey

	Perform vulnerability survey	 
	Check the security assumptions regularly during life-time	 

Security updates

	Protect the software update mechanism	
--	---------------------------------------	-------------------------------------------------------------------------------------

Remote interfaces protection

	Provide user-friendly interfaces for device and services security management	 
	Protect remote monitoring interfaces	 

Security management system for support infrastructures

	Rely on existing sources for security good practices in order to secure infrastructures	 
--	-----------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Control of user data

	Provide secure backup and/or deletion of the data stored/processed by the device (and by associated cloud services) during the operation and at end-of-life	 
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Annex D: Example of topics for user awareness

This annex presents an example of possible actions to perform in order to:

- Choose a Smart Home device securely
- Operate a Smart Home device securely
- Use online services for Smart Home securely

HOW TO CHOOSE A SMART HOME DEVICE SECURELY

Verify if the smart features are really required or if a normal device would be sufficient
Be careful when buying used IoT devices, as they could have been tampered with
Research the vendor's device security measures
If battery powered, favour devices providing alternate/emergency charging methods

HOW TO OPERATE A SMART HOME DEVICE SECURELY

Change default password of Wi-Fi networks and use robust encryption (e.g. WPA2)
Change default password of device
Disable or protect remote access to IoT devices when not needed
Use wired connections instead of wireless where possible
Modify the privacy and security settings of the device to your needs
Disable features that are not being used
Install updates when they become available
Use devices on separate home network when possible
Ensure that an outage (for example due to jamming or a network failure) does not result in a unsecure state of the installation

HOW TO USE ONLINE SERVICES FOR SMART HOME SECURELY

Use a password manager
Use different passwords for different services
Control data exchange requested by a service

Annex E: List of Acronyms

ACRONYM	DEFINITION
AFR	Annual Failure Rate
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
APT	Advanced Persistent Threat
ASLR	Address Space Layout Randomization
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CERT	Computer Emergency Response Team
CPA	Commercial Product Assurance
CSPN	Certification Sécuritaire de Premier Niveau
CO ₂	Carbon dioxide
CPU	Central Processing Unit
CSA	Cloud Security Alliance
CSRF	Cross-Site Request Forgery
DMA	Direct Memory Access
DTLS	Datagram Transport Layer Security
DoS	Denial of Service
EC	European Commission
EU	European Union
FTC	Federal Trade Commission
FTP	File Transfer Protocol
HAN	Home Area Network
HDL	Hardware Description Language

HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HW	Hardware
I2C	Inter-Integrated Circuit
IBC	Identity-Based Cryptography
IBE	Identity-Based Encryption
IDS	Intrusion Detection System
IoT	Internet of Thing
IPC	Inter-Process Communication
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISP	Internet Service Provider
ISP	In-System Programming
JHAS	JIL Hardware-related Attacks Subgroup
JTAG	Joint Test Action Group
JTEMS	JIL Terminal Evaluation Methodology Subgroup
LED	Light-Emitting Diode
LPWAN	Low-Power Wide-Area Network
MNO	Mobile Network Operator
MS	Member States
MTBF	Mean Time Between Failures
MVNO	Mobile Virtual Network Operator
NAS	Network Attached Storage
OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
OS	Operating System

OTA	Over The Air
PCB	Printed Circuit Board
PCI	Payment Card Industry
PKI	Public Key Infrastructure
PIN	Personal Identification Number
R&D	Research and Development
RFID	Radio-Frequency IDentification
SaaS	Software as a Service
SMS	Short Message Service
SoC	System on Chip
SPI	Serial Peripheral Interface
SSL	Secure Sockets Layer
SSH	Secure SHell
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TV	TeleVision
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPS	Wi-Fi Protected Setup
XSS	Cross-Site Scripting



ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



TP-04-15-834-EN-N



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-141-0
doi:10.2824/360120

