TRAFICOM
National Cyber Security Centre

Date: 2-12-2020

Statement of compliance for the Cybersecurity Label

Contact information

Company name:	Signify

Structure and Directions

The goal of this form is to provide information on the security of an IoT product to NCSC-FI as well as technically inclined users. The form is published as a part of a consumer material kit when a label is granted.

Chapter 1 lists general information of the IoT product and the surrounding ecosystem such as mobile applications and cloud services provided by the vendor or third parties. The sections of chapter 2 list security threats that are relevant to consumers as well as security requirements that, when met, mitigate these threats. Where possible, the requirements are accompanied by tables that may be used as part of the response. Some descriptive texts for describing the security posture of the product are suggested.

The ETSI references within the text are related to provisions in the standard ETSI TS 303 645 "CYBER; Cyber Security for Consumer Internet of Things". The final draft (v2.1.0, 2020-04) is available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf.

1 Product Description

Describe the product or product family (the "Product") under application, along with ecosystem provided by the vendor or third parties (the "Service") that is relevant for core functionalities of the Product.

Philips Hue is the world's leading connected lighting system for the home. It comprises smart bulbs, strips, spots, lamps, and controls to create the perfect ambiance for any occasion. The system is transforming how light is used in and around the home to stimulate people's senses, light their moments and help provide peace of mind when away from home.

1.1 Support Period

An end-of-life policy shall be published for the Product that explicitly states the minimum length of time for which it will receive software updates (ETSI 4.3-4). For constrained devices that cannot have their software updated,

the product should be isolable and the hardware replaceable. The period of hardware replacement support and an end-of-life policy should be published. (ETSI 4.3-8, 4.3.9)

The Hue bridge is designed to be connected to the internet. The Hue bridge receives software updates directly from Signify (formerly known as Philips Lighting) when connected to a router with internet access and used with the official Hue mobile application.

Signify intends to provide your Hue bridge with major platform feature software updates, if any, for a minimum of one (1) year from the date of your purchase from an authorized reseller (except in cases where the hardware is not capable).

In addition, Signify intends to continue to support the Hue bridge with required security, quality and interoperability updates as well as maintaining compatibility with our online services and the latest version of our mobile Hue application for a minimum total of three (3) years from the date of your purchase from an authorized reseller.

After these dates, Signify may choose to continue to provide software updates and/or compatibility with online services and/or mobile applications at its discretion. Should software updates and/or compatibility with online services and/or mobile applications however be terminated, we recommend you upgrade to a new version of the product.

Please visit the following web-page for detailed information per product-type: https://www.philips-hue.com/fi-fi/support/end-of-support-policy (in Finnish).

1.2 Security Guidance

Security guidance for the Product is available in Finnish at http://example.com/vendor/security/Product (ETSI 4.12-1).

Hue product do not require security configuration; they are secure by default. Security advisories (FAQs) can be found here: https://www.philips-hue.com/fi-fi/support/security-advisory (in English, currently no Finnish version is available).

1.3 Other Certifications

The product has a CE marking. The product has certification X (e.g. the UK security label, provide link). The service components of the product have been verified by Y (provide link), or have certification Z (e.g. the STAR certification from the Cloud Security Alliance, provide link).

Signify implements a secure software development lifecycle, which has recently been certified against the IEC 62443-4-1 standard by DEKRA.

Issued by:	DEKRA Certification B.V.
Reference no:	NL-65080
Type:	Process Capability Assessment
Certificate Coverage:	New Product Development and Launch Process for connected Lighting Systems Version 2.7
Requirements Assessed:	Security Management (13/13), Specification of Security Requirements (5/5), Secure by Design (4/4), Secure Implementation (2/2), Security Verification and Validation Testing (5/5), Management of Security-Related Issues (6/6), Security Update Management (5/5), Security Guidelines (7/7)
Standard(s) used:	IEC 62443-4-1:2018
Issued date:	2020-4-15

Go to https://certificates.iecee.org/ods/cb_hm.xsp and type "NL-65080" in the Free text search field.

Hue products are GDPR compliant and internally validated against IEC 62443-3-3 Edition 1.0 - System security requirements and security levels.

Hue cloud uses Google Cloud Platform which holds several certifications. See https://cloud.google.com/security/compliance for a complete overview.

2 Protections Against Common IoT Threats

The Product has protections for common IoT threats as described by the sections below.

2.1 Weak, Guessable, or Hardcoded Passwords

All IoT device passwords shall be unique and shall not be resettable to any universal factory default value (ETSI 4.1-1).

Describe how the Product is protected against the threats caused by weak or hardcoded passwords. As an example, if the threat is compensated by using security controls beyond identification, or if user identification does not use passwords, describe how the resulting security level is equal to using strong and unique passwords.

To control your Hue lamps remotely the Hue bridge must be linked to a Hue cloud user account. The account registration process requires the user to enter a personal password that is subject to a password policy, which ensures that the entered password meets our quality requirements. On our security roadmap for early 2021 are (amongst others) support for two-factor authentication.

2.2 Use of Insecure or Outdated Components

All software components in the Product should be securely updateable (ETSI 4.3-1). The consumer should be informed that an update is required

(ETSI 4.3-2). Updates shall be timely (ETSI 4.3-3). The need for each update should be made clear to consumers and an update should be easy to implement (ETSI 4.3-5). The vendor shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues (ETSI 4.2-1).

Describe how the Product and Service are protected against the threat of insecure or outdated components. As an example, describe how vulnerability follow-up is performed throughout the supply chain for all the components, including operating systems, network services and software libraries. Describe how timeliness, ease of installation, quality control and secure transfer and installation is ensured in updates of the Product. Typical update cycles range from 30 to 90 days, though this may vary greatly depending on the nature of the product.

To ensure that software is not released with known vulnerabilities, Signify uses packet managers to keep open source components up-to-date. In addition, a tool (WhiteSource) is used to scan for known vulnerabilities. Reported vulnerabilities (including those that are reported via the Signify responsible disclosure program) are assessed and, depending on the determined risk-level, prioritized for mitigation by means of an emergency release or a scheduled maintenance release. In 2020 the Hue bridge has a monthly release schedule.

Vulnerabilities are mitigated thru an over-the-air software update service. Software update files are digitally signed, allowing mobile phones, Hue bridges, and Hue lamps to determine the integrity and authenticity of the software update before installation. Hue bridges are updated using a Signify operated service that can reach +90% of all connected Hue bridges within 48 hours. Hue lamps are updated over the Zigbee network thru a connected Hue bridge.

When the user has not disabled the Hue automatic update service, no user intervention is required to keep their Hue products up-to-date.

Signify manages "security in the supply chain" thru contracts containing a "security schedule". The security schedule stipulates the supplier's obligations with respect to security. This includes (amongst others) the obligations to warn Signify in case of a security incident involving their product or service and to provide security updates in an agreed timeframe based on severity. Suppliers of online services are also required to have an industry recognized security certification like SOC or HITRUST.

2.3 Insufficient Privacy Protection

Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers (ETSI 4.8-1).

Describe how it is ensured that the handling and storage of personally identifiable information within the Product and the Service is performed in a

manner that is transparent to the user and limited to the extent necessary for providing the functionality.

The Signify corporate privacy office signs-off on GDPR compliance. This process is repeated every time new features are introduced. The Hue mobile application asks the user for consent on data collected using opt-in and opt-outs. Data is subsequently anonymized or stored securely in the Hue cloud.

The privacy policy (see link below) provides an overview of personal data stored by Hue devices, Hue mobile applications, and the Hue cloud.

https://www.philips-hue.com/fi-fi/support/privacy-policy (in Finnish).

2.4 Insecure Data Transfer and Storage

Security-sensitive data, including any remote management and control, should be encrypted in transit, with such encryption appropriate to the properties of the technology and usage (ETSI 4.5-1). All keys should be managed securely (ETSI 4.5-2). Credentials and security-sensitive data shall be stored securely within services and on devices (ETSI 4.4-1).

Describe how the Product and the Service, as well as the communication between the Product and the Service, are protected against the threats caused by lacks in data encryption and access control. For protecting passwords, this typically includes the usage of hash functions.

The Hue bridge accepts incoming HTTP and HTTPS connections from within the local network from applications that have been previously authorized by the consumer by pressing a button on the Hue bridge.

HTTP support for third party applications that do not yet implement HTTPS will be discontinued in 2021. A sunset for these legacy applications is already announced to the Hue developer community in 2020. Nonetheless, customers using the official Hue mobile application and bridge can be rest assured that all communicated data is protected using HTTPS.

The Hue bridge initiates outgoing HTTP and HTTPS connections on the remote network interface. All connections use HTTPS to protect the integrity and confidentiality of data exchanged. There is one exception: the Philips device management service uses HTTP in combination with a proprietary, application-level security layer, which has been extensively reviewed and pen-tested by external partners. The Philips device management services will be renewed in 2021 after which HTTPS supported will be added and enforced.

The Hue cloud uses a PKI which allows Hue bridges and Hue mobile applications to verify the authenticity of the cloud service. The Hue bridge uses a private PKI which allows Hue mobile applications to verify the authenticity of the bridge service. The Hue mobile application uses access tokens to authenticate itself to the Hue cloud and Hue bridge.

2.5 Insecure Network Services and Ecosystem Interfaces

Unused software and network ports should be closed (ETSI 4.6-1). Software should run with least necessary privileges, taking account of both security and functionality (ETSI 4.6-5). Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated (ETSI 4.13-1).

Describe how the Product is protected against the threats caused by the vulnerabilities in the exposed network services such as web interfaces and remote management. Also consider the used radio interfaces.

Describe how the exposed network interfaces in the Service, are protected against threats such as unauthorized access and breaches of confidentiality. These interfaces are typically related to functionalities such as the cloud-based data storage and management of the Product.

You can use the following table in your response to sections 2.4 and 2.5. Listing the tools and methods used to test the Product and the Service will help in their evaluation.

The Hue bridge is designed to not require ingress connections to function. Therefore, no port forwarding on the customer's router is required to control your Hue products making the Hue bridge undiscoverable on the Internet.

The Hue bridge implements a web server, which is kept up to date using a package manager. The configuration of the web server is benchmarked against industry best practices using a software tool (CIS benchmarks).

The Hue bridge is hardened thru input validation and the application of a firewall. All unused protocols and services are removed from the firmware image.

The Hue mobile application and Hue cloud services run in restricted accounts and sandboxes. The Hue bridge and Hue lamp firmware execute under a single unrestricted account.

Network port / Radio technology	**Encryption / access control**	**Usage**
Ethernet (Hue bridge)	HTTPS, access tokens, physical access.	The Hue bridge does not support Wi-Fi IP connectivity, only ethernet.
Zigbee (Hue bridge, Hue lamps, Hue accessories)	According Zigbee specification.	Distributed Zigbee network. Additonal measures: Proximity commissioning with time-out. Opening of the commissioning window after first-use requires physical access.
Bluetooth (BLE) (Hue lamps)	According Bluetooth specification.	BLE JustWorks profile and BLE Link Layer Encryption. Additional measures: Proximity pairing with time-out. Opening of the pairing

Network port / Radio technology	Encryption / access control	Usage
		window after first-use requires physical access to the device.

2.6 Insecure Default Settings

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability (ETSI 4.12-1).

Describe how the Product and the Service are protected against the threats caused by insecure factory or default settings. Also describe how the user is guided to maintain a secure configuration.

Hue products are designed to be secure by default. Users are not required to make any security decisions. The automatic software update function is enabled by default, which ensures the users that the latest software with the latest security patches is running on their products.

Hue bridge and Hue lamp configuration settings (not visible to the user) are reviewed before product release. In addition, each new Hue product is subject to a pen-test to uncover (amongst others) possible configuration errors.

Hue cloud configuration settings are periodically benchmarked against industry best practices using a software tool (CIS benchmarks).