interact

Security

Architecture PRF/PRA

Version v2.4

4 August 2023

Contents

1. Introduction

PRF/PRA is a connected lighting system combining connected luminaires, sensors, and other lighting system devices with Interact software and services like apps and portal. PRF/PRA system devices connect to the Internet and embed two-way data communication with cloud-based services: a such they participate in the Internet-of-Things (IoT). With the proliferation of these devices in buildings, it is key to address the security risks associated with its use. With this document, we address security risks, implementations, processes and responsibilities.

Security is embedded in all aspects of our innovation, products, systems, and services—from secure system development, to device, network and cloud security, system monitoring, and secure device updates.

Our security processes are built on a strong PRF of industry standards, governance, and procedures. When selecting Signify as a partner for PRF/PRA , you can trust that we have dedicated abundant attention to security across all of products, systems, and services, and that Signify will support you throughout the entire lifecycle of PRF/PRA .

2. Implementation of security principles

All of our internal and external development activities follow the Signify Security Development Lifecycle (SDL), which codifies industry accepted best practices. The major components of the SDL are security risk analysis and threat modeling, code analysis and review, and vulnerability management. We apply the SDL to all of our hardware products, systems, services, software, and cloud solutions.

In accordance with the SDL, Signify takes the following actions during design, development, and testing:

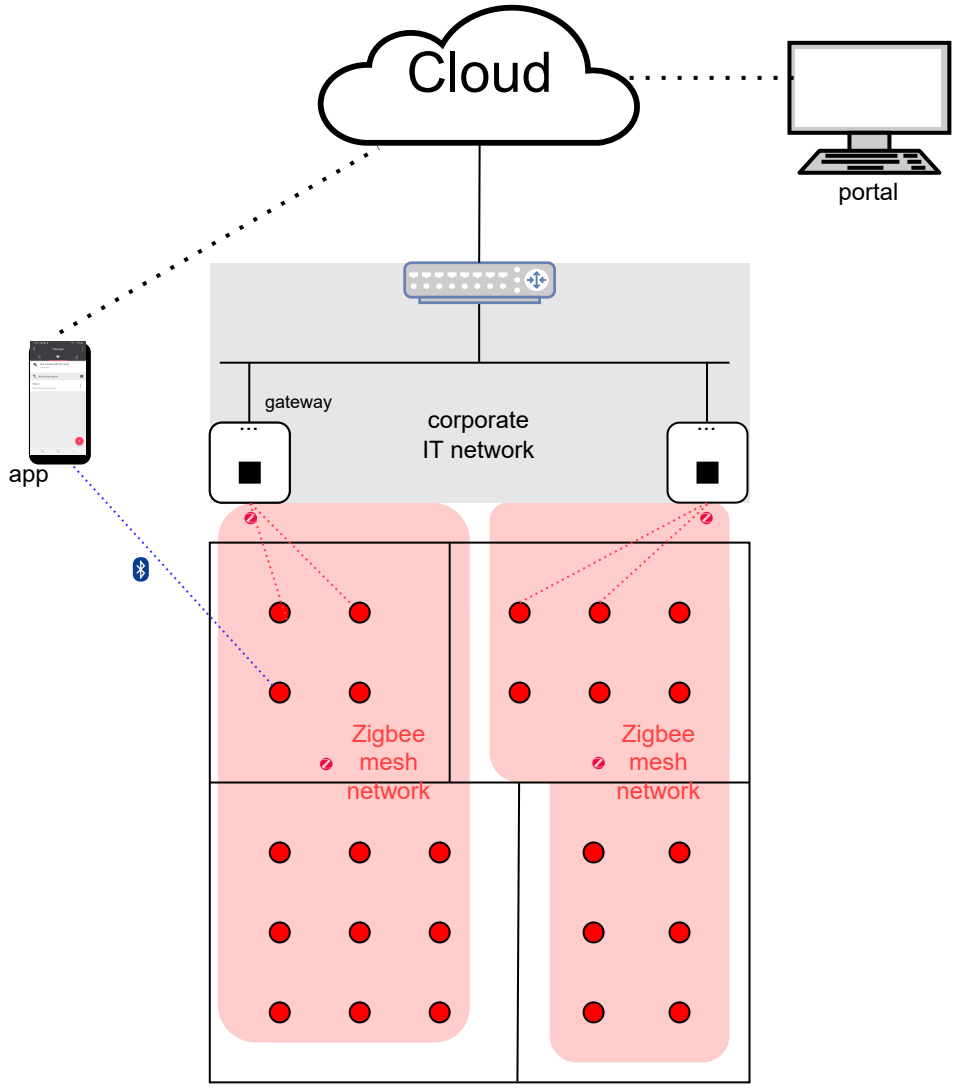
- A security risk analysis, based on Signify security requirements aligned with the ISA/IEC 62443 standards suite, is performed for every new project and for every significant change to an existing project.
- Automated code analysis and manual code reviews are regularly performed during development. These analyses and reviews are based on, but not limited to, such frameworks as OWASP IoT Project and the OWASP Top Ten Project.
- Third-party code, including open source code, is automatically analyzed to identify and mitigate vulnerabilities.
- Hardening of the operating system is performed for embedded devices and cloud-based solutions.
- Appropriate network security and firewall rules are implemented and reviewed regularly.
- Encryption of data in transit and at rest is implemented according to generally accepted industry standards as described in the Federal Information Processing Standard Publication 140-2 (FIPS 140-2).
- Penetration tests are performed before each customer release by internal teams and external parties at a minimum of once a year.

The Innovation team is responsible for evaluating the latest IoT security technologies, and supports the development team in making the right choices when introducing new security algorithms, solutions, and technology partners.

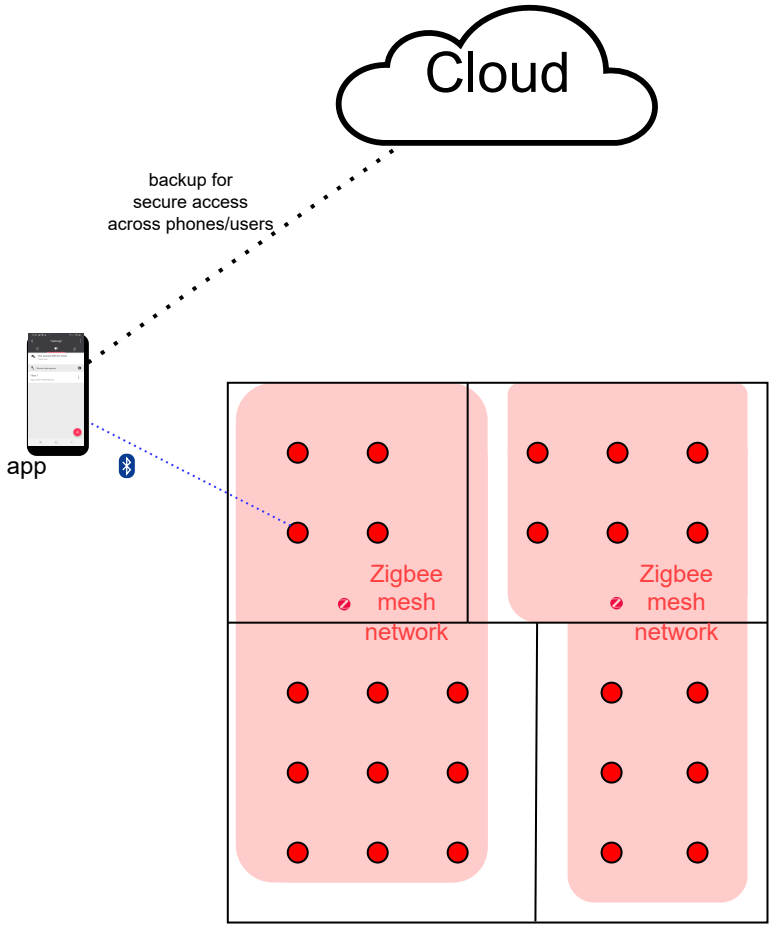
Signify regularly audits its partners and supply chain to maintain the appropriate level of security in the manufacturing process.

3. Architecture and security

The figure below depicts an overview of an PRA system.



The overview for PRF:



In PRF or PRA, light control is implemented using a wireless mesh network based on the Zigbee protocol: two-way communication between lights and discrete controls is solely based on this protocol. Commissioning and user control are done using a mobile phone app.

When the system is connected to the internet via gateways:

- Bluetooth can be used for two-communication between the phone and individual lights for commissioning.
- Lighting control is enabled via the gateway: the phone communicates via the cloud with the gateways and the gateways (edge devices) communicate with the lights via Zigbee.

For connected systems, each gateway is the trust center for all the other Zigbee devices in the network it is connecting to.

When the system is not connected via gateways:

- Bluetooth is used for two-communication between the phone and individual lights for commissioning and control: the phone connects to a light via Bluetooth and information is shared across lights using the Zigbee protocol.
- Essential security data is backed up in the cloud to enable secure transfer of access rights to the system to other phones and authorized users.

For non-connected systems, the mobile phone serves as the trust center for each light network it can connect to.

In both cases, non-connected and connected, system security is addressed end-to-end to guarantee data confidentiality, integrity and availability: to ensure this, network security, device and physical security, communication security for in-transit data, cloud security as well as installation security aspects are addressed.

4. Network security

Various encryption techniques are used to ensure that all communication is protected end-2-end between devices used in an PRF/PRA system. To protect the PRF/PRA cloud services, only Interact devices can access them. This is ensured by using unique device credentials that are assigned to all devices during production. The identities of all of these devices are maintained in the cloud platform. Only devices with a known credential can communicate with PRF/PRA cloud services.

All communication between devices on-site and the cloud is done by PRF/PRA gateways. This communication is encrypted using the standard TLS1.2 protocol. Authentication ensures that only these Interact devices are communicating with our cloud services. Furthermore, all communication is enabled inside out: that is the gateway connects to the cloud rather than the other way around.

Gateways do not store data: they relay data coming from other devices to the cloud. To optimize communication and to bridge periods with limited connectivity they may temporarily store some data in memory. However, they are connected to the customer's IT network and have ample computing and memory resources. To prevent tampering with gateways, that they can't be used to compromise the customer network or access data, they are hardened to minimize attack surface and vectors.

Wireless lights, sensors and switches are communicating using the Zigbee protocol. This protocol uses a 128-bit AES key to encrypt messages for protection. This key is unique to each Zigbee network and generated randomly at the creation time of the network.

The PRF/PRA app can directly communicate with the latest generation of wireless devices that besides Zigbee also allow for Bluetooth communication (only between mobile devices and an Interact device). Bluetooth security builds on the security libraries of the operation system of the supported mobile phone platforms, iOS and Android. The complete security solution consists of:

- a Signify specific implementation of a key exchange protocol using the standard NIST SP 800-56A C(2e, 2s) ECC CDH : Elliptic-curve Diffie-Hellman using two static keys and two ephemeral keys (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf) where ECC used P-256 curves.
- PRF/PRA -specific Bluetooth messages are encrypted with a standard AES CCM crypto algorithm using a 256-bit AES key

5. Device and physical security

All device features and requirements are aligned with the OWASP IoT framework and built with security in mind. The devices' Operating Systems are hardened by whitelisting of services and libraries.

Firmware updates are started using the app or portal by authorized users. All firmware images are signed and verified before being deployed on end devices.

5.1. Wireless Gateway (LCN1840/05)

The gateway is a bridge between the Zigbee devices in the lighting network and a wired network using an Ethernet interface. Via this interface, it communicates securely with the Interact cloud platform. They have the following security features:

- Hardened operating system
- Non-availability of hardware debug interfaces
- Disabled user login
- Secure updates via signed firmware images
- Encrypted communication
  - using TLS to communicate over the internet with the cloud
  - using encrypted Zigbee to communicate with the light network

5.2. Light and control devices

Lights, sensors and switches are based on electronic devices that perform two-way communication in the lighting network using Zigbee. The mobile app can also directly communicate with a Bluetooth-enabled device.

They have the following security features:

- Non-availability of hardware debug interfaces
- Disabled user login
- Secure updates via signed firmware images
- Encrypted network traffic
  - using Zigbee to communicate between system devices
  - using Bluetooth to communicate between mobile app and system devices

6. Cloud services

The cloud platform is key component of PRF/PRA :

- For PRA, the lighting system is normally 24/7 connected to it for remote access and monitoring.
- For Foundation, it is used as a backup for security credentials that are required to access the system. Without such a backup, transfer to other phones and users is impossible. Security is given top priority to make sure that data is protected against unauthorized access and that the cloud services can only be accessed by authorized users (including devices communicating with the cloud).

6.1. Encryption and key management

PRF/PRA uses only NIST-approved encryption algorithms ensuring that only strong cryptographic algorithms are used:

- Data in-transit between a gateway and the cloud platform is encrypted using TLS1.2
- Zigbee network traffic is using the Zigbee security mechanisms as defined in IEEE 802.15.4. Messages are encrypted using a unique 128-bit AES key (each Zigbee network has its own unique key.
- For Bluetooth communication between a mobile phone and Bluetooth enabled lights a solution is used based on a key change protocol using the standard NIST SP 800-56A and messages are encrypted using AES CCM crypto algorithm with a 256-bit key. The implementation builds on crypto libraries provided by iOS and Android OS.

6.2. Business continuity

High availability of cloud services is an important objective. For PRF/PRA cloud services, an architecture with a redundant system with automated failover is implemented. Availability target of cloud services is over 99%. Historically, the last year availability has been close to 100%.

PRF/PRA has a 24/5 service time, that is service is available throughout the day world-wide on regular business days. The operations team reacts within 4 hours for incidents where the service is down, and 1 business day on for minor incidents. Outside service time, only an emergency service is available and the response time will be 24 hours.

Backups are available to be able to recover to a point in time. Backup data is kept for 1 month for the primary backup. An additional backup is kept with a retention time of 1 year.

6.3. Authentication and authorization

PRF/PRA uses an identity management system to control access to the cloud. It manages user accounts and the privileges or roles for those accounts. Pending on the role, a user has access to one or more projects and to specific functionality in the system. A user can access a project securely after login with his credentials on the mobile PRF/PRA app or the PRF/PRA portal on the web.

Gateways also use the identity management system when they connect to the cloud using unique device specific credentials. These credentials are securely stored on each device as part of the production process. The process is documented and following strict security requirements on handling this data. It is supervised by a dedicated security officer.

To identify gateways when they are added to a project, its unique MAC address can be captured by the mobile app. This associates a unique device (with unique credentials) with the project it is added to. Access to this project is only allowed by authorized users of that project.

6.4. System updates

The PRF/PRA cloud is updated regularly to ensure that security vulnerabilities are dealt with in a timely manner. Before deploying an update, a new release is tested at various levels to ensure data consistency and to prevent accidental data modifications. As part of the test process, security tests are executed for every release.

Security issues, when they are discovered, will be prioritized over the development of functionality to guarantee that a patch is deployed quickly mitigating the issue. Release procedures guarantee that such an update can be made available without impacting quality.

7. Security installation requirements

PRA gateways communicate with the cloud via a customer's IT network using IPv4. Each gateway needs to receive an IP address from a DHCP server on that network. The use of static IP addresses for gateways is not possible.

All connections from PRF/PRA devices to cloud services are initiated by the gateway using dedicated URLs and ports. New connections created outside the network are not allowed. Secure communication is always initiated by a gateway of an PRF/PRA system. Communication between the gateways and the cloud uses the HTTPS protocol which uses the standard TCP port 443. MQTT messages are also sent using this port. The benefit is that only standard web browser ports need to be opened up for PRF/PRA devices to communicate with the cloud.

The URLs and ports used by PRF/PRA are:

- sme.interact-lighting.com for port 80 and 443
- mq.sme.interact-ligthing.com for port 443

Optionally, when allowed on the customer's IT network, UDP port 123 needs to be open to allow for NTP (Network Time Protocol) time synchronization.

These URLs and ports need to be whitelisted using the security framework of customer's IT network to allow for communication between PRF/PRA gateways and the cloud.

Note that PRF/PRA PRF doesn't impose any requirements on the customer's IT network. Only the phone used for setup and control of the system needs to be able to connect to the cloud platform for backup purposes.

8. Operations

At Signify, we implement a security policy which enforce segregation of duties and least privilege access.

The PRF/PRA cloud services are managed by a specialized global operations team to ensure proper segregation of duties for system administration purposes. Responsibilities of the team include producing operational specifications and performing maintenance, security updates, vulnerability management, backup, logging, monitoring, and management of events and incidents. The team also performs periodic review of network and application security. Development teams and in general other personnel do not have access to production systems or production data. In case access to data is necessary, for supporting operations, only the Operations team is allowed and strictly for the limited time and scope needed.

9. Privacy and data governance

PRF/PRA application services (mobile app, and PRF/PRA web portal for PRA) are managed by the concept of **Projects**. A Project is characterized by (part of) a building at a specific location and dedicated user account(s). Data of different projects are separated from each other. All data of a project is considered confidential.

Data of all Projects (except China) is stored with the following cloud provider at the following locations:

- AWS region Europe (Frankfurt) - Germany
- Device registration of LCN1870 gateway: AWS region Europe (Ireland)- Ireland

For reliability and availability, backups are stored at two different locations to be able to recover from a major system event.

Data is stored in the form of

- database entries on servers
- system generated emails
- log files
- backups
- login account data

Project data can only be accessed by authorized users or Signify user managers via user accounts. User accounts are created through self-registration, which results in a profile having project ownership and by invitation, which results in a profile giving a user the necessary rights to access the project data via its application services. PRF/PRA supports different user profiles with associated access rights and capabilities for its application services.

Project data consists of system telemetry and personal identifiable information, each of which will be processed differently (see also 'Data processing').

For more information on Signify's privacy and data governance, visit our privacy notice page.

9.1. System telemetry

System telemetry data can be divided a number of categories:

- Asset data about deployed systems, their devices and settings such as types, power consumption, work processes and all kinds of customizable data fields.
- Operational data about the operational use of the deployed systems including metric data like energy data, system error messages and service availability.
- Log data about the events in the system.

Backup data of the operational productions system.

PRA stores system telemetry data in the cloud to enable remote access and dashboard functionality. For PRF, no system telemetry data is stored to the cloud. Optionally, the app can create a log file of events which is stored securely on the phone: this data has to be explicitly shared by the user, for instance for support reasons.

9.1.1. Light source, driver and sensor data

Smart lamps, wireless drivers, drivers and sensors are nodes in a Zigbee mesh network. A project is composed of one or more of these Zigbee networks. Devices in these networks relay data from one to another for control purposes. When used, gateways are also an integral part of these Zigbee networks and metric data of devices is sent via the mesh network to the gateway which sends it to the cloud (see next section). All communication in a Zigbee network is encrypted using AES with a unique 128-bit key.

The following data is shared:

- Motion data
- Light level data
- Firmware version
- Failures
- Power consumption

9.1.2. Edge devices (gateways)

Gateways relay telemetry data received from devices in the mesh network to the cloud. A gateway also sends log data to the cloud for monitoring of health status. All communication between the gateway and cloud is sent using MQ Telemetry Transport (MQTT) using TLS1.2 encryption.

Gateways do not store data. Only when a connection is down, they buffer data and will sent that data to the cloud when the connection is restored.

9.2. Personal Identifiable Information (PII)

Personal Identifiable Information is stored in various data categories:

- User accounts to get access to the system
- Technical log data that stores events in the system among which are user actions in the UI
- Security log data that stores essential user actions, needed for security analysis of system access.

To get access to the system, a user needs to minimally supply (self-registration) or accept (invitation) using a valid email address used to create a user account. The following information is captured:

- Name
- Email address

(Optional) Contact information

- (Optional) Phone number
- (Optional) Address data
- Country

For PRF, the email address and project are used to create a security certificate. This is important to be able to protect the system against unauthorized use by thirds. And also to be able to guarantee continuity, this data is backed up in the cloud: to extend access to other users and for use on other mobile devices.

For PRA , the data is stored securely in a protected database in the cloud.

The app allows automatic retrieval of location data provided that the user explicitly permits to use *location services*.

9.3. Data processing

Signify ensures that the use of system telemetry data excludes any Personal Identifiable Information. Signify only processes Personal Identifiable Information in accordance with Signify Privacy Notice. The Signify "Privacy Notice for Customers, Consumers and Other Business Persons is available on http://www.signify.com/global/privacy under the "Legal information" section.

The list of processing purposes for Personal Identifiable Information that are relevant are

- Assessment and (re)screening of (potential) Customers, Suppliers and/or Business Partners
- Conclusion and execution of agreements
- Providing support
- Security and protection of our interests/assets
- Compliance with legal obligations and Defense of legal claims
- Product development

Signify will protect all Data adequately using industry standard technical and organization measures, such as encryption (depending on the nature of the Data), restricted access to the Data only on a need to know basis, etc.

9.3.1. Customer rights to access data

In case a customer requests access to Personal Identifiable Information or prefers to exercise its individual privacy rights they need to contact the Signify Privacy Office via https://www.signify.com/global/privacy/privacy-request.

Signify will grant the customer access to (non-personal) system telemetry data in accordance with the customer contract.

10. Standards

Signify policies and processes are aligned with global standards such as ISO/IEC 2700x—Information Security Management Systems (ISMS) and the ISA/IEC 62443 standards suite for product development. Signify is **IEC-62443-4-1** certified which ensures that development and maintenance processes enable the creation of secure systems.

Through our Standards and Regulation department, we collaborate with many worldwide standardization organizations, such as IEC, ANSI, and CENELEC, and with industry alliances such as the IoT Security Foundation.

Signify also aligns its practices with the Cloud Security Alliance (CSA) self-assessment tool.

Signify business processes are internally and externally audited on a regular basis.

11. Shared responsibility

Signify recognizes that the security of our products and services is an important part of our customers' in-depth security strategy. In practice, however, security is a responsibility shared by manufacturers and providers of products and services and their customers.

Appropriate evaluation of risks and proper care in installation, maintenance, and operations are essential to mitigate internal and external threats.

For PRF/PRA , the following practices are customers' responsibility:

- Always update PRF/PRA app and system devices to the latest version in particular when a release addresses a security issue.
- Users have access to an PRF/PRA system using one or more accounts created by self-registration or invitation and as such they are fully accountable for all actions taken under these accounts. It is recommended to follow common security practices for the creation and management of passwords.

12. Reporting security incidents

Security incidents for PRF/PRA are to be reported via its support channels, either the local support call center or the Customer Satisfaction team of the market.

Signify supports responsible vulnerability disclosures and encourages researchers and ethical hackers to report identified vulnerabilities. For more information on Signify responsible disclosure, visit the vulnerability disclosure page.

13. Legal disclaimer

This information is provided for informational purposes only. It represents the current product information as of the date of publication. These are subject to change without notice.

Customers are responsible for making their own independent assessment of Signify products or services and the use thereof. This information is provided “as is” without warranty of any kind, whether express or implied. This information does not create any warranties, representations, contractual commitments, conditions, or assurances from Signify, its affiliates, suppliers, or licensors. The responsibilities and liabilities of Signify and its customers are defined in the agreements between Signify and its customers. This information is not part of, nor does it modify, any agreement between Signify and its customers.

Learn more about Interact
www.interact-lighting.com