

Network Architecture and Data Flow



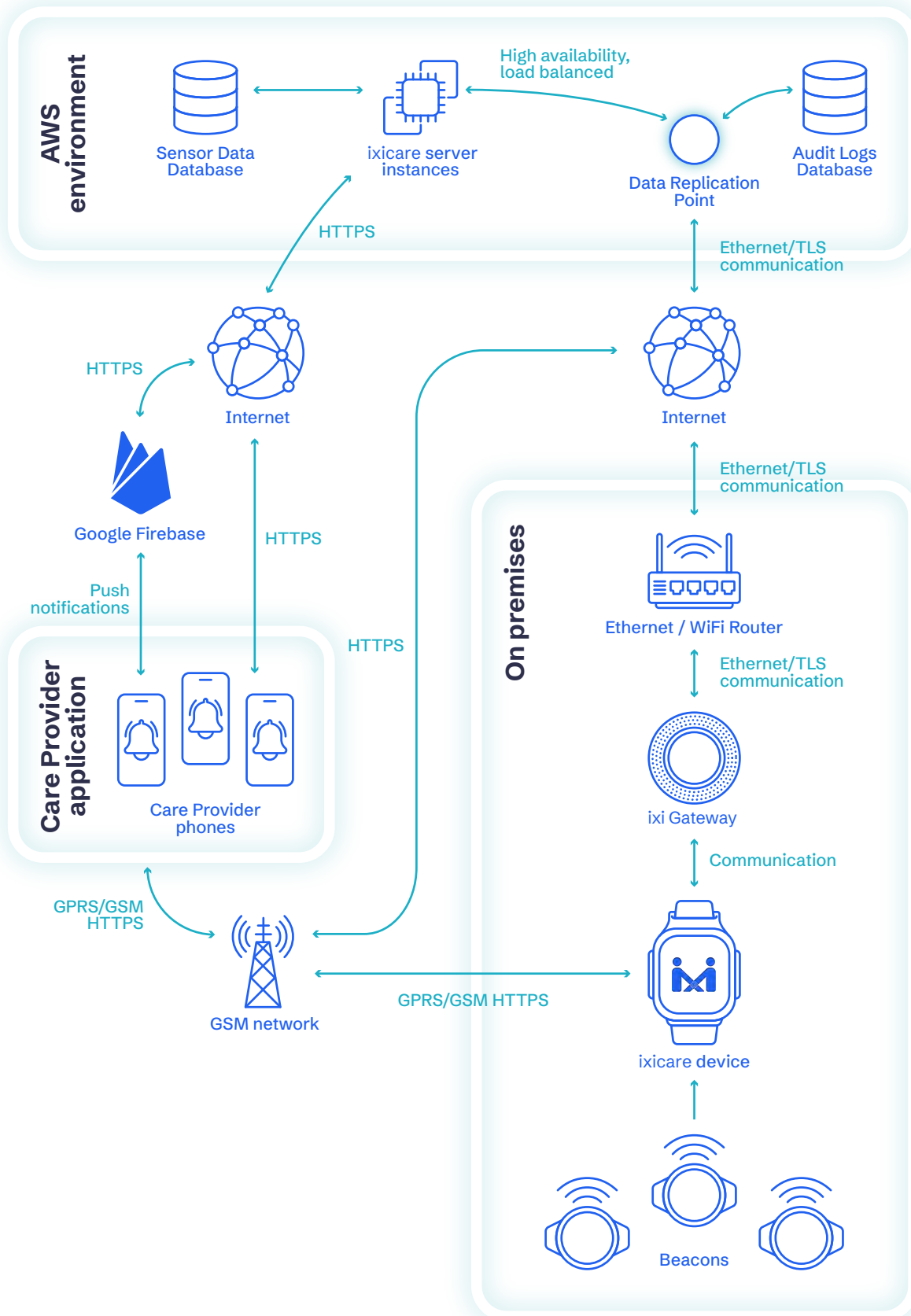


The purpose of this document is to provide in-depth information of the network topology, architecture, networking components and security aspects of the ixicare service.

Contents

Overview	4	Cloud/AWS	10
Description	5	Key components of the cloud/AWS domain	10
On-premises	5	ixicare server instances	11
Key components of the on-premises domain	5	Managed database service	11
ixicare wearable and wall devices	6	Managed load balancers	11
ixicare wearable and wall devices – Network	7	Alert management	12
ixicare wearable and wall devices – Data	7	Key components of the alert management domain	12
ixi Beacons	8	Alert management application	13
Power failover solutions	8	Push notifications	14
Internet gateways with failover capabilities	8	Platform Integrations	14
Data Transfer	9		

Overview



Description

The ixicare service consists of three discrete domains:



The On-premises domain



**The cloud/
AWS domain**



The alert management domain

These domains have different runtime and security characteristics, as well as different High-Availability attributes.

On-premises

This domain consists of the ixicare wearable devices, wall buttons and ixi Gateways. It is complimented by Wireless/wired routers that allow the ixicare device traffic to be transported securely to the network and the cloud service, as well as power failover solutions (such as UPSs) that allow the operation of the network service even in the event of a power failure. Additionally, it benefits from smart routers that can switch from the landline to a 4G connection, to allow continuity of service operation in the event of a landline network failure.

Key components of the on-premises domain



ixicare wearable and wall devices



ixi Beacons



ixi Gateways



Power failure fail-over solutions



Internet gateways with failover capabilities

ixicare wearable and wall devices

These devices consist of the sensors that continuously receive readings such as Location, the manual alert systems (Buttons) and the modems that allow the wearable devices to transmit their readings to the backend cloud system.

The ixicare Lite and the Wall button devices have been designed for indoor usage, frequency hopping 2.4Ghertz radio technology.

The ixi Pro device has the additional capability of using the GPRS/ GSM connectivity to allow data transfers over the cellular network and receive voice calls during an emergency.



Works indoors & outdoors



Waterproof IP68



2-way SIM Communication



Geolocation during alarm



Manual alerts with a touch of a button



Smartwatch can be worn while charging



Long battery life

...and many other readings and features.

ixicare wearable and wall devices - Network

The devices send their data to the network every few seconds, depending on their power profile.

The data use the inherent security scheme when connecting to the ixi Gateways, coupled with a custom layer of security that identify the devices as ixicare devices and prevent any spoofing attacks to the network (use of a signature to prevent impersonation attacks).

Moreover, the devices apply a layer of encryption to the transmitted data, to protect them from eavesdropping (in case an attacker impersonates an ixi Gateway).

The data encryption is applied end-to-end and uses unique credentials per device, so that if one device is compromised, it won't expose the rest of the devices in the field.

ixicare wearable and wall devices - Data

The devices are associated with their wearers (or residents), therefore the sensor data are also inherently associated with identifiable people.

The data is not processed or permanently stored inside the ixi Gateway or the Network Routers, and they are transmitted using TLS encryption over TCP to the cloud services (TLS v1.2). An additional layer of encryption and validity signature protects the data end-to-end (based on SHA256 and AES256).

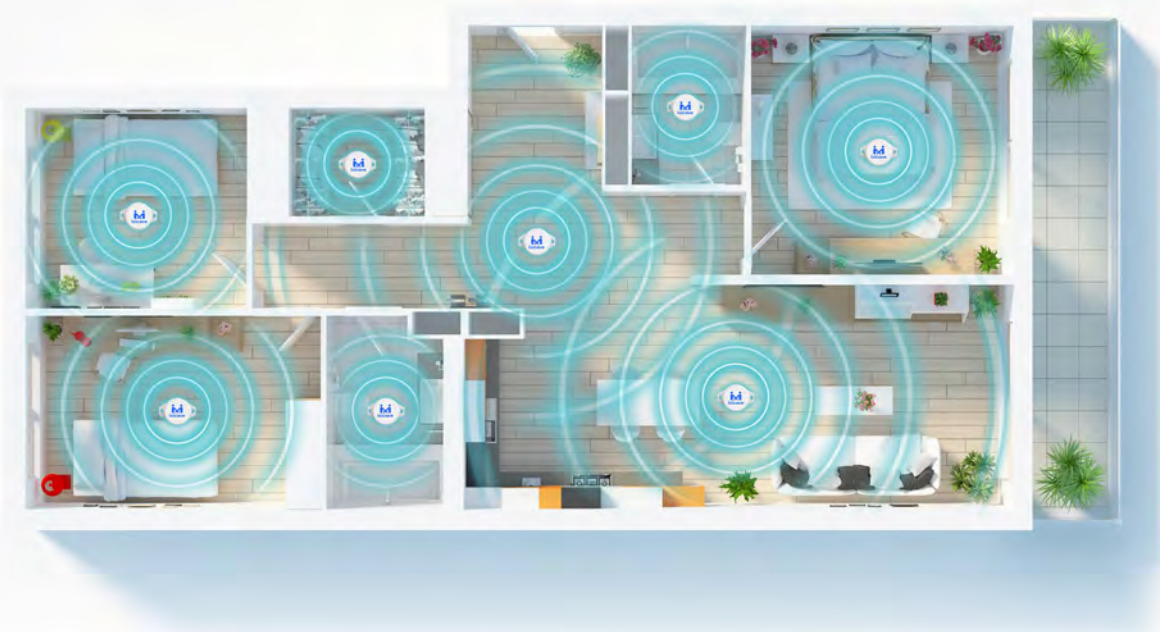


ixicare Beacons

The beacon devices are used to identify indoor areas (or to a certain degree nearby outdoor) and complete the InterLocation Tracking capabilities of the ixicare service.

The beacons are broadcasting a proprietary pattern that identifies them as ixicare devices. The beacon MAC addresses are pre-registered in the backend system to avoid simple impersonation or spoofing attacks.

Additionally, the ixicare service has the intelligence to identify scenarios where a beacon is “moved” or is reported to be in the vicinity of other beacons that are not supposed to be nearby.



Power failover solutions

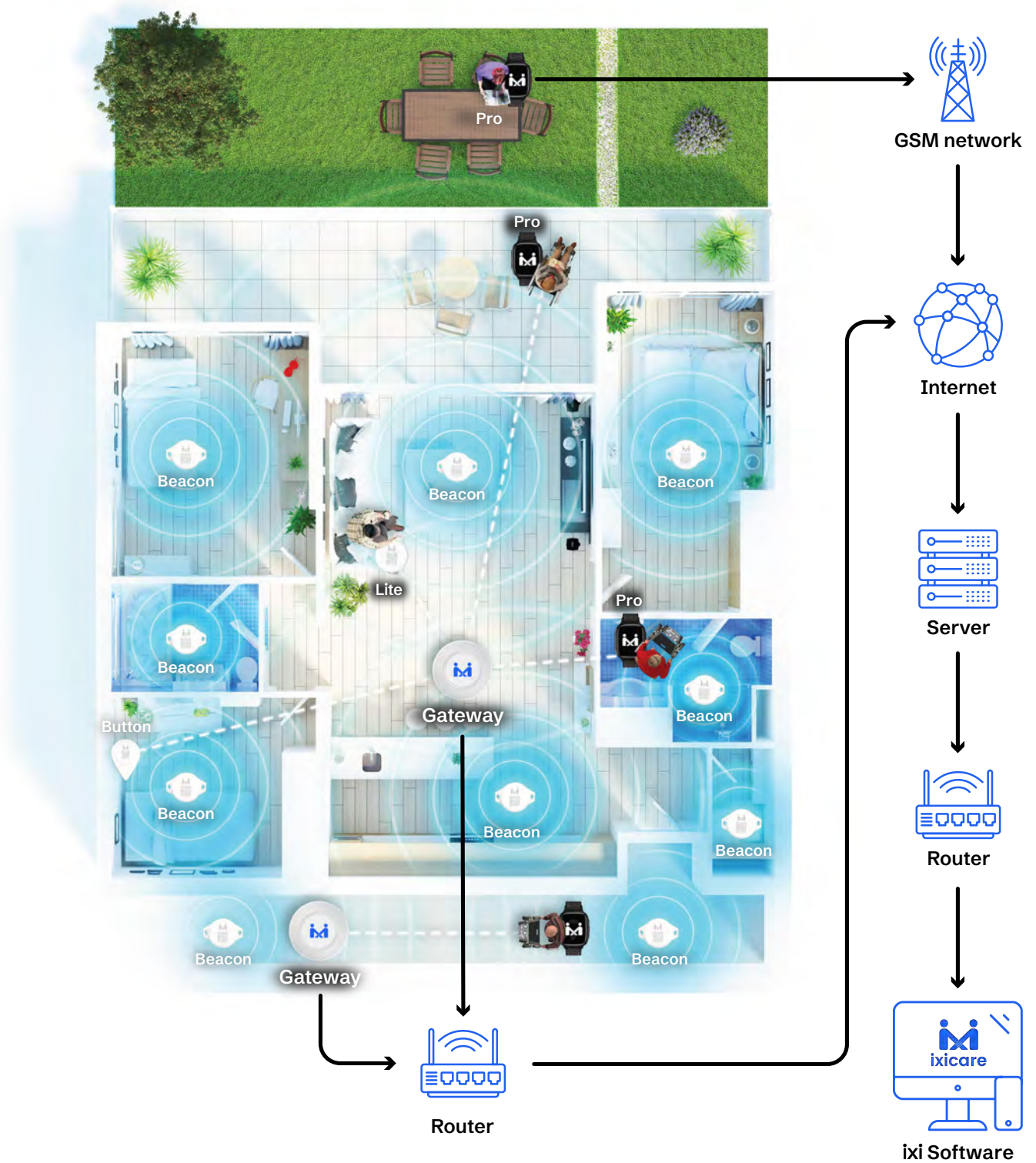
The ixi Gateways are often deployed using Power-Over-Ethernet solutions, to reduce the number of cables and to have a central switch to control the data and power supply. The power to the switch is monitored by UPS systems that allow for an uninterrupted operation for some time depending on the UPS system.

Internet gateways with failover capabilities

The ixicare service requires continuous connectivity to the Internet and the cloud services that process the sensor data. The gateways that offer the Internet interfaces have the ability to switch to a wireless/cellular network if the connectivity over the landline is interrupted.

Data Transfer

The ixicare system works indoors via the client's local area network and the ixicare bluetooth grid, whereas in outdoor environments the ixi Pro connects to mobile networks via a SIM card.



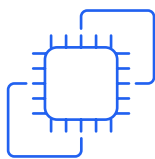
Cloud/AWS

The ixicare service resides mostly in a cloud environment, using AWS infrastructure to perform the processing of the sensor data, classification and storage. The environment is hosted in European datacenters, using encrypted disk drives for the transient data that are processed by the ixicare server instances and the managed databases (encrypted disks for the data at-rest).

The cloud environment uses a virtual network, isolated from the rest of the cloud tenants in the datacenter by enforcing a virtual private network topology. The cloud network is protected by a managed firewall that limits the access to the ixicare servers and blocks direct access to the databases (the databases can be accessed only by the internal servers and not by external applications via network ports).



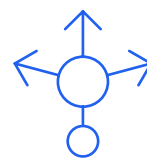
Key components of the cloud/AWS domain



ixicare server instances



Managed database service

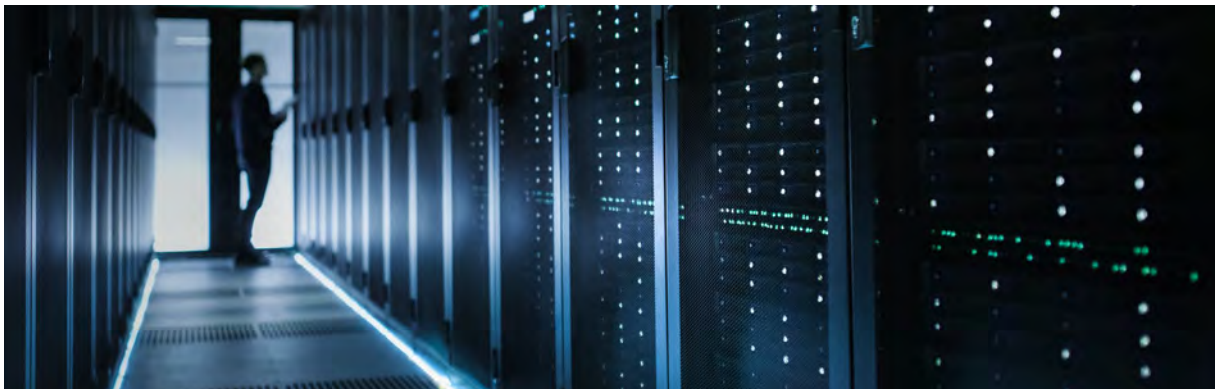


Managed load balancers

ixicare server instances

The server instances handle all the requests from the devices and the nurse applications. They implement the core service logic, following a high-availability scheme with multiple instances being available to process the incoming requests. If some of the instances stop working, the system will raise an alarm to notify the Ops and will temporarily compensate by dynamically distributing the incoming requests to the remaining nodes.

The access to the server instances is audited and limited to only security cleared personnel.



Managed database service

The ixicare service uses a managed database solution to store the sensor data of the devices associated with the device wearers. ixicare has full ownership of the data, so this database is used to store the raw data as well as any data that is derived from the processing of raw sensor data.

The access to the database service is audited and limited to only security cleared personnel.

The database service is fully managed with redundancy, so that the data is always protected from disasters in the same cluster of the datacenter. ixicare also performs frequent data backups to ensure that there is no loss of data in the event of a catastrophic failure in the datacenter.

Managed load balancers

The ixicare service uses load balancing between the ingress and egress servers to be able to accommodate changes in the load of the incoming and outgoing data and also to handle potential service failures in a graceful manner.

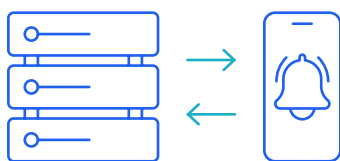
Alert management

The alerts and the user-facing ixicare service management system is provided to the authorized personnel (as well as the maintenance crews) via Role-Based Access control scheme.

The authorized users have their own unique credentials that are managed by ixicare and they can access the parts of the service only by using their credentials, for a short period of time (after a few hours the service access times out and requires the users to login again). ixicare also supports integration with Identity Provider systems (e.g. via OAuth2, OpenID).



Key components of the alert management domain



ixicare alert management application

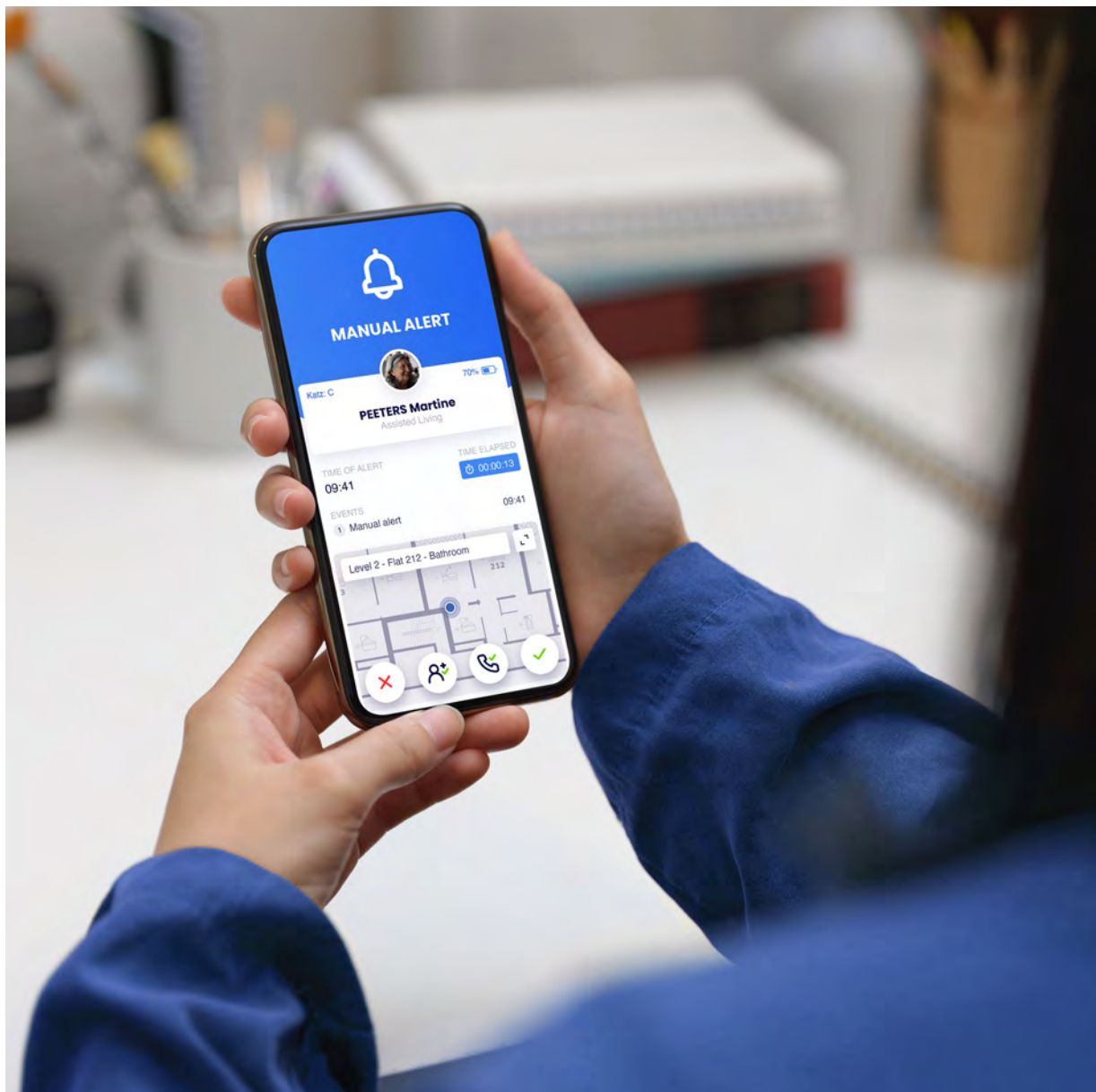


Push-notifications

Alert management application

Alarm management access to the ixicare service is provided via a mobile app that receives real-time updates from the ixicare servers regarding alarms and location information of the ixicare device wearers. The information is exchanged between the ixicare servers and mobile devices over an HTTPS connection, which carries encrypted and signed data (using an additional layer of security on top of the TLS 1.2 layer) to eliminate the possibility of impersonation attacks or DNS spoofing.

No data is stored permanently on the mobile devices that run the ixicare alert management application.



Push notifications

To ensure the success of reporting new alert incidents, the ixicare service uses multiple notification paths. The push notifications complement the incident reporting mechanism, by sending notifications to the mobile device app that will be delivered to the mobile device regardless of the running status of the ixicare application (e.g. if a member of the staff has accidentally stopped the application from running).

The push notification information does not include any specific details about the new incident, but informs the user that there's a new event that needs his/her attention. The push notification service guarantees the identity of the originator of the messages with the use of pre-shared secrets and private/public encryption mechanisms, to eliminate impersonation attacks.

Platform integrations

ixicare is a software cloud platform where different systems such as hardware and software can be integrated or connected to either via changing the firmware on the devices or via the backend.

Due to an open API-structure, ixicare can easily connect to medical and non-medical systems.





Contact

support@ixicare.com

Warande 13B

9270 Laarne, Belgium

www.ixicare.com