CONTACT
HARALD

Contact Harald
Card Technical Specifications

Version 1.2.4

Abstract

This document describes the technical description, specifications and performance of the Contact Harald Cards for the Contact Harald System (**System**).

It is part of a suite of documents that should be read and used together including:

Product Warranty and Use
Card Button Press and LED Status
Card and Battery Safe Disposal.

This document is for general circulation, suitable for general technical audiences.

Version Control

Document Version	Version 1.2.1 1.2.2 1.2.3 1.2.4
Date	7 April 2021 8 April 2021 14 April 2021
Author/Owner	MattD, MorganL
Update	Minor updates and corrections.

Document Version	Version 1.2.0
Date	4 and 5 March 2021
Author/Owner	MattD
Update	Separate out Card Specifications from older Technical Specifications document with all products.

Table of Contents

Card Bluetooth Specification

The Contact Harald Card is a Bluetooth 5.0 Low Energy device, as defined by the Bluetooth specification. Bluetooth operates at 2.4Ghz.

Bluetooth Low Energy uses very low power radio waves and has been designed to work in most common work and home environments without significant interference.

https://en.wikipedia.org/wiki/Bluetooth_Low_Energy

Please check if your facility has special requirements, such as sensitive medical measurement equipment.

Card Dimensions and weight

Size: 3.38” x 2.13” x 0.16” (86 mm x 54 mm x 4 mm)
Weight: 0.635 oz (18.0 g)

Card rating – water, dust resistance and testing

The Card internal electronics are protected using an ultrasonic welded plastic housing.

The battery and electronics are sealed inside the unit.

The Card is rated at IP66: the enclosure is dust tight and is water resistant against water projected from a nozzle.

The Card has a drop test rating of IK05.

Battery Specification and Performance

The battery is 800mAh 3V, LiMnO2, non-rechargeable cell. The battery cannot be replaced.

Once the Card is commissioned and registered, the Card is always on. The only exception is Visitor Cards: a Visitor Card is turned off once it has been checked-out through the System.

The battery is designed to function continuously for **approximately six months**, depending on usage. Factors include operating temperature or temperature fluctuations, number of uploads and general load on the Card.

See separate document **Product Warranty and Standard Use** for further details.

When the battery is low, the LED light on the Card will blink before expiry. Typically the LED light will blink slowly at approximately 5.5 months, then blink faster at approximately 15% remaining battery. At 10% the Card will sleep to preserve power, permitting an upload of records from the Card. A battery report is available from the online System. It requires an upload to get an accurate reading of the battery (it will give a battery reading from the last Card upload). If required, please order a replacement ahead of time.

See separate document **Card Button Press and LED Status** for further details.

To safely dispose of the Card, see **Card and Battery Safe Disposal** for further details.

Please Note: Contact Harald offers other options and product form factors, with different performance characteristics. Please ask for further information, if needed.

Normal Operating Temperatures

The Card is designed to operate in normal indoor environments and temperatures.

The Card is design to operate between 5 ℉ to 131 ℉ (–15 ℃ to +55 ℃) temperature bands. Storage temperature –4 ℉ to 140 ℉ (–20 ℃ to +60 ℃). Outside these temperature bands, the Card may not function correctly, or the internal electronics or battery may fail.

If your facility has harsh temperature conditions or large temperature fluctuations, we advise you to consult with our team to discuss the System performance.   Note at –4 ℉ (–20 ℃) or lower the battery performance is about half.

See separate document **Product Warranty and Standard Operation** for Standard Operation.

Proximity Contact Records

To understand who was in close proximity with who, the Contact Harald Card records when two or more Cards are nearby, using bluetooth radio signals as an **approximate measure of distance**.   If the radio signal or RSSI is within a threshold, the two Cards are considered close together. The Cards are calibrated to use a series of RSSI measurements to approximate six feet or 1.5 metres of each other. Environmental and interference factors may affect the RSSI and thus the accuracy of the measurements and the classification of a close contact.

Two or more Cards exchange anonymous ID numbers. No personal information is shared between the Cards. The anonymous IDs are rotated every 15 minutes to avoid potential tracking or monitoring of the Cards using Rotating Proximity Identifier (RPI).

If a User has symptoms or a positive COVID result or is informed of a trace to a positive COVID result, it is the User's responsibility to inform the organization that gave him or her the Card of such information and that organization is responsible for uploading that information to the Application (including via Bluetooth to an iPad or Gateway), which then transfers via the Internet to the secure database. Without this information being notified by the User and uploaded promptly and accurately then the data retrieved from the Card by the organization will be affected, and your contact tracing program will not work optimally. The Card data contains anonymous IDs that can be matched to other Users.   The other Users who have been traced can be immediately contacted and asked to test and self isolate.

Contacting other Users

The Contact Harald System can identify the close contacts then send SMSs or emails to each traced person, or provide a list to management to immediately manually contact trace.

Proximity Contact Distance and Time

The System has been configured to measure and rank contacts within approximately six feet or approximately 1.5 metres of each other. Bluetooth signal strength, or RSSI is used to approximate distance.   The Cards have been calibrated to work best when worn on the lanyard around the neck or clipped to the front of the body. When Cards are worn on other parts of the body or carried elsewhere, this reduces the performance and the chance of accurate contact trace.

When two Cards come within six feet proximity of each other for two minutes or more, a contact event is saved on the Card.   Multiple contacts are tallied up to give a total contact time. For example, if two people were together for four minutes, then apart for a while, then back together for six minutes the System would display a total of ten minutes cumulative time.

Due to Bluetooth performance and potential environmental and radio signal interference, a confidence ranking is also applied to the proximity time. In ideal conditions, the System will give good confidence.

Card Memory Storage and Privacy

The Card is designed to store 20 days of proximity contacts. As COVID-19 may be pre-symptomatic or asymptomatic, 20 days gives historical data to trace back through earlier contacts.

Card Cryptography

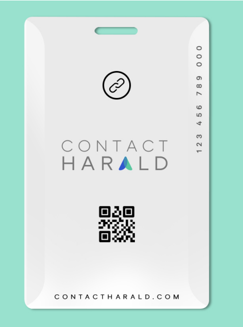
The Card uses onboard AES 128 cryptography to generate a random Rolling Proximity Identifier (RPI) every 15 minutes.

Database Storage and Privacy

By default, the database is designed to store 20 days of proximity contacts. As COVID-19 may be pre-symptomatic or asymptomatic, 20 days gives historical data to trace back through earlier contacts.

Aged historical proximity data is deleted from the Contact Harald database. The age of the proximity records is a configurable number of days set in the Application by the System administrator at your organization; the default is set to 20 days and the maximum setting is 1,095 days (ie. three years).

Card Identification numbers



Each Card has two unique markings:

The Card ID number runs along the top right hand edge, a 12 digit number. This is a unique identification to the Card and is not associated with a person until the Card is commissioned. Once commissioned, no personal information is stored on the Card, only a uniquely generated number.

The QR-code is the same as the unique ID number, used to save typing the 12 digit number into the System.   The registration protocol lets you use the camera on the iPad or other device to scan the QR-code in, entering the Card ID number.

Contact Harald System Components

The Contact Harald System is broken down into three primary components, and three optional components:

1. Contact Harald Cards.
2. An iPad or equivalent (containing the Application) that is used to register Users and associate the Bluetooth Contact Harald Card to the System.   The iPad is also used to upload Card proximity data to the System via Bluetooth.
3. The Microsoft Azure database and contact tracing web-application which operates in the Safari and Chrome web browsers.
4. **Optional** Gateways to automatically capture and upload card proximity data to the contact tracing database. Triggers are supplied with the Gateways to prepare or ‘prime’ cards for an upload as a user approaches a Gateway.
5. **Optional** Beacons to detect ‘presence’ for location check-in technologies replacing QR-code manual check-in.
6. **Optional** Remote Upload of the card data via an iOS app or Android app. This is a secure, upload-only function. It must be enabled first by Contact Harald; it is supplied with separate instructions.

iPad Registration and Card Upload

The iPad and Application is designed to register new Users and associate the unique Card number to the User. The Application can also collect data from the Card via Bluetooth and store it on the secure online database server.

This data is uploaded securely to the Microsoft Azure database. No personal data is stored on the Card. The Application is designed to be easy to use.

The iPad can be used by staff with low security clearance, for example a temporary reception staff member. The staff member does not have access to the database and cannot lookup User data.

Secure Microsoft Azure Database and Contact Tracing System

When a User registers with the System (via the Application), their data is securely stored on a Microsoft Azure server. A secure link is established between the local web-based local session and the cloud-based server.

Only authorized Users can access the personal data to run or run a contact trace based on a User's proximity information. Different levels of authorization give different access levels to the System and such authorizations are made by the organization who manages and issues the Card to Users (eg: the customer, not Contact Harald).

Email and SMS

Twilio is used to send out SMS messages to end users. A secure connection is established between the Twilio service and our end point. Message Send status is passed back to our App, which is logged to each SMS message, which in turn is logged to a User.

SendGrid, part of the Twilio family and used to send emails out to end users. Similarly, a secure connection is established between the SendGrid service and our end point. Email Send status is passed back to our App, which is logged to each email message, which in turn is logged back to a User.

Due to automation of this messaging, the System relies on the accurate and up-to-date uploads of information. We ask that System administrators at our Customers' organisations manage this in a diligent and timely manner.

Personal Data, Privacy and Storage

No medical data is stored on the System by us. When a User self-reports, a record of such is kept without specific details of the medical condition or status. All personal data is encrypted and stored on the secure Microsoft Azure database. Personal data for a User is accessible by the System administrators at the organization which issued the User the Card. If a User has any privacy issues in respect of the Card, please contact the organization which issued the Card.

When registering the Card for the User, the User consents to the collection of their name and contact details, certain data being held regarding that User and their proximity data being collected, uploaded and used by the System for the purpose of contact tracing (typically after the User reports positive to a test, reports that he or she showing symptoms of a possible infection, or reports that he or she has been contact traced elsewhere).

The Contact Harald System records and stores proximity information for contact tracing purposes (such as when cards record a trace with each other and when a card records its presence with a beacon), however outside of these traces we do not track User location data.

Additionally, our Customers may request location check-in technologies from us (eg. QR codes) to record a person's entry to a site area. Our Customers have the ability to use opt-in protocols with these. If requested by the Customer, beacons can be used to provide automatic and seamless check-ins, removing the need for individuals to manually "scan-in" (eg. using a QR code) on entry to a site area.

Beacons record will 'presence' for a check-in however they do not continuously track a card location. This check-in data may be called upon by a relevant local health authority via a designated API. Access to such data requires the relevant authority to place a request that is permitted under relevant privacy legislation. Beacon information is stored on a card, the card data is passed up to a Gateway and then to the secure database.