NHS COVID App

Overview Diagrams
External system linking with Privacy

May 2020

Licensing & Usage

This document describes the Bluetooth proximity contact tracing application built by VMware Pivotal Labs for the UK Government.

NHSX

Overview

The Proximity Tracing App is a privacy ensuring service with no PII linking whatsoever. User research has shown that the more PII this application is linked to, the lower the uptake and usage of this app.

For these reasons we must have a way of allowing people in the app to ‘link out’ to other NHS services. These services may request more PII but that should not be stored in the Sonar backend. Conversely, the SonarID should not escape the Sonar backend in order to prevent others from linking in the future.

The external system though may wish to notify the Sonar backend that the use of this code is complete, and the status of the user has changed (E.g. positive/negative test result) - but no PII.

This presentation describes a privacy preserving mechanism built on the concept of a one time use reference code for each interaction with an external service elsewhere in the NHS.

Approach for IoW phase Privacy protecting reference code

User clicks ‘show my reference code’.

This is displayed to the user E.g. **ab5f-h38d**

1.1

Additional data never goes in to Sonar - interaction happens outside of the app

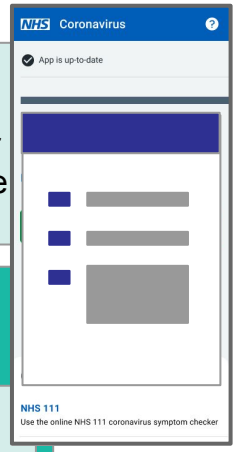
App Back-end

1.1: App contacts NHS Sonar backend to generate a temporary reference code for their Sonar ID.

Approach for national launch reference code

Security: External system gateway needs to ensure a request cannot be misused to check for a valid reference code in Sonar.

User clicks a link in the app for a specific function, or requests a one time use code



In embedded browser

Code passed, and other data from user requested.

Additional data never goes in to Sonar - it's outside of the app

1.2

External System Gateway

2.2

Other systems ...

1.1

2.1

2.3

2.4

App Back-end

1.1: App contacts NHS Sonar backend to generate a temporary reference code for their Sonar ID.
1.2: App passes this reference code via the phone's web browser to the external gateway service. The user interacts with this page.

2.1 Gateway verifies this is a valid Reference Code with Sonar backend. (May not be done, subject to security note above)
2.2 Reference code may be passed to other backend systems
2.3: Gateway sends a status change to the Sonar backend that is useful for its function (E.g. test result positive/negative and date) along with the one time use reference code.
Sonar back-end destroys the reference code once results verified, or once it times out, removing any ability for PII linking between Sonar and NHS systems
2.4: (Optional) Depending on scenario, the back-end may send a notification to the main proximity tracing app

NHSX

Display of the reference code

The code will be displayed in the Mobile App for the Isle of Wight phase as an alpha-numeric set of digits.

We are using Crockford's Base 32 to generate a visual alphabet. This eliminates the characters I, L, O and U. This helps prevent the commonest confused characters and the generation of accidental obscenity.

An example code:-

6db8-2hjt

This is lowercase for readability.

We were unable to remove some potentially confusing letters (e.g. 2 being confused with an uppercase Z) because we need at least 32 characters for encoding.

This functionality may be retained for future versions, including national roll out, based on need.

How the value is constructed

How a value is created:-

- A value is constructed using a secure random number generator
- The first 35 bits are taken
  - This results in a 2^35 address space = 34 359 738 368 values
- A 5 bit checksum is constructed using a Damm algorithm and appended to the data bits. (This can be easily used to check validity in excel)
- Giving a total size of 40 bits

How the resultant data is displayed and used:-

- 5 bits = 1 visual character using a 32 bit alphabet (Because 2^5 = 32)
- This gives 8 characters to cover the full 40 bits
- This will be returned as a lowercase alphanumeric hyphen separated string
- The linking code will be temporary (E.g. up to 2 weeks old), and deleted upon expiry
- For external system linking (E.g. testing) the code will expire upon first use
- We ensure that they are unique in the database