COVID EXPOSURE NOTIFICATION OUT IN THE OPEN

An Open Implementation of the Google/Apple Exposure Notification Protocol

David Llewellyn-Jones, Jolla Oy

FOSDEM

5th February 2023

jolla

SAILFISH OS

Covid Exposure Notification Out in the Open

COVID EXPOSURE NOTIFICATION OUT IN THE OPEN

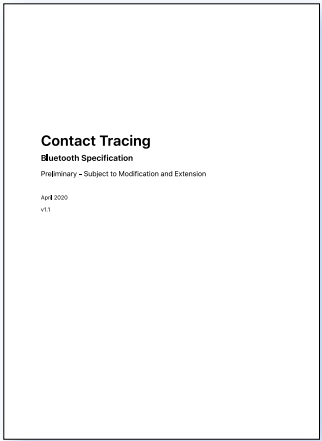
An Open Implementation of the Google/Apple Exposure Notification Protocol

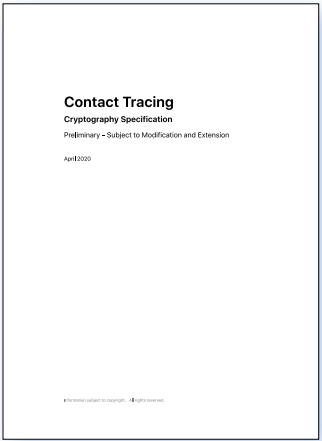
David Llewellyn-Jones, Jolla Oy
FOSDEM

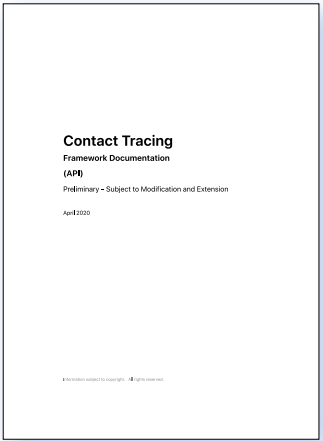
5th February 2023

1. Who am I?
2. Who do I work for?
3. What does Jolla do?
4. What is Sailfish OS?

GAEN



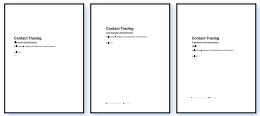




jolla

SAILFISH OS

GAEN

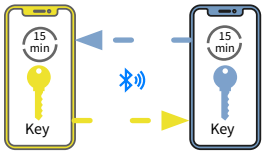


The Google/Apple Exposure Notification API

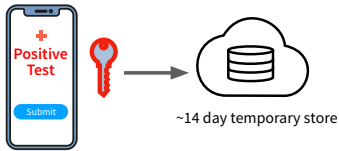
1. Version 1.1 released April 2020
2. At that point it was still called the "Contact Tracing" framework
3. Made up of three documents [1]:
   - 3.1 Framework Documentation (API)
   - 3.2 Cryptographic Specification
   - 3.3 Bluetooth Specification
4. Privacy-focused
5. Works using Bluetooth and backend servers run by state-level organisations

GAEN

1. Alice and Bob meet
Their phones exchange frequently changing anonymous identifier beacons

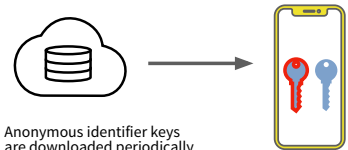


2. Bob is positively diagnosed
With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud



Apps can only get more information via user consent

3. Alice receives a warning
Alice's phone periodically downloads beacon keys of everyone who tested positive in her region; a match is found with Bob's anonymous beacons



Anonymous identifier keys are downloaded periodically

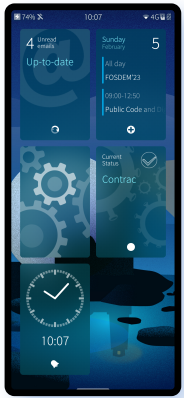
A match is found

jolla

SAILFISH OS

1. At this point in time the world was in a state of shock and panic.
2. There was no vaccine.
3. Avoiding *contact* to reduce the R number was the main aim.
4. Some countries had already introduced contact tracing apps
   4.1 *e.g.* South Korea's *Corona 100m app* using GNSS in February 2020 [2].
5. Governments were clamouring to do something similar, but there were privacy concerns.
6. **Android and iOS provided the on-phone capabilities, but not the cloud infrastructure.**

SAILFISH OS



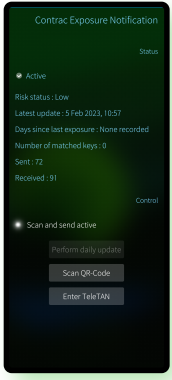
SAILFISH OS

jolla

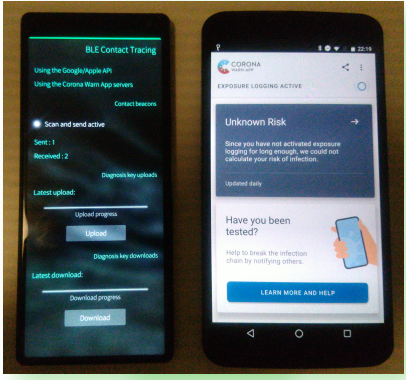
SAILFISH OS

1. GAEN was a big deal.
2. Google and Apple realised the significant risks involved.
   - 2.1 Privacy risks of governments violating privacy.
   - 2.2 Efficacy risks of having multiple systems.
   - 2.3 Reputational risks of their platforms being used badly.
   - 2.4 Their APIs already prevented this for privacy and power reasons.
3. The GAEN system was very robust from a privacy perspective.
   - 3.1 Decentralised up to the point of positive diagnosis.
   - 3.2 Frequently rotating unlinkable identifiers.
   - 3.3 Matching performed on-device.
4. My concern, as a Jolla employee, was the danger of Sailfish OS users being sidelined.

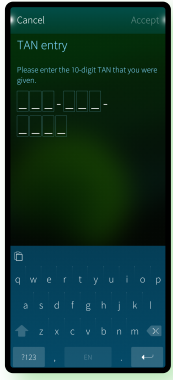
CONTRAC



Contrac app



Scanning and sending



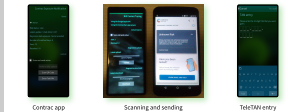
TeleTAN entry

jolla

SAILFISH OS

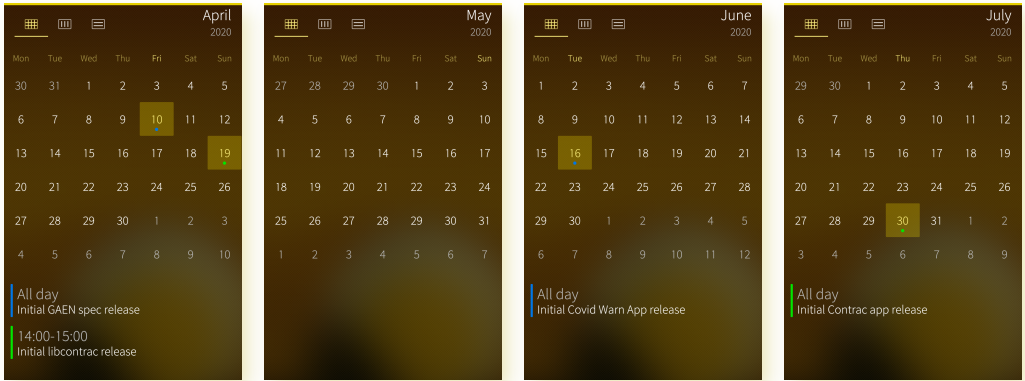
Covid Exposure Notification Out in the Open

└Contrac



1. Germany's Covid Warn App alternative.
2. Built in collaboration with Oskar Roesler.
3. Independent of Jolla.
4. Open source, Qt, Bluez, OpenSSL.
5. Background service for Bluetooth control and computation (GAEN part).
6. Front-end for control, upload and download (Covid Warn App part).

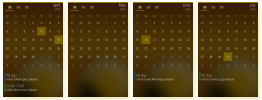
TIMELINE



jolla

SAILFISH OS

TIMELINE



1. Time was critical and we wanted to be responsive.
   1.1 10 April 2020: GAEN specification release
   1.2 19 April 2020: Initial GAEN library release [3]
   1.3 16 June 2020: First Covid Warn App release
   1.4 30 July 2020: First app release [4]
2. It felt like a success, but wouldn't have been possible without:
   2.1 Early release of high quality GAEN specs.
   2.2 Early release of good quality CWA documentation.
   2.3 Release of an example server was critical.
   2.4 Release of sourcecode was useful for edge cases, but not critical.
3. Some of the server implementation had to be derived from the documentation.

WORKING WITH GOOGLE AND APPLE

A great job with the design, specs, API but no collaboration

1. No direct interaction
2. Specs provided early
3. The promised test data never materialised
4. Relevant code not released until too late
5. Nevertheless, the specs were good enough to implement

jolla

SAILFISH OS

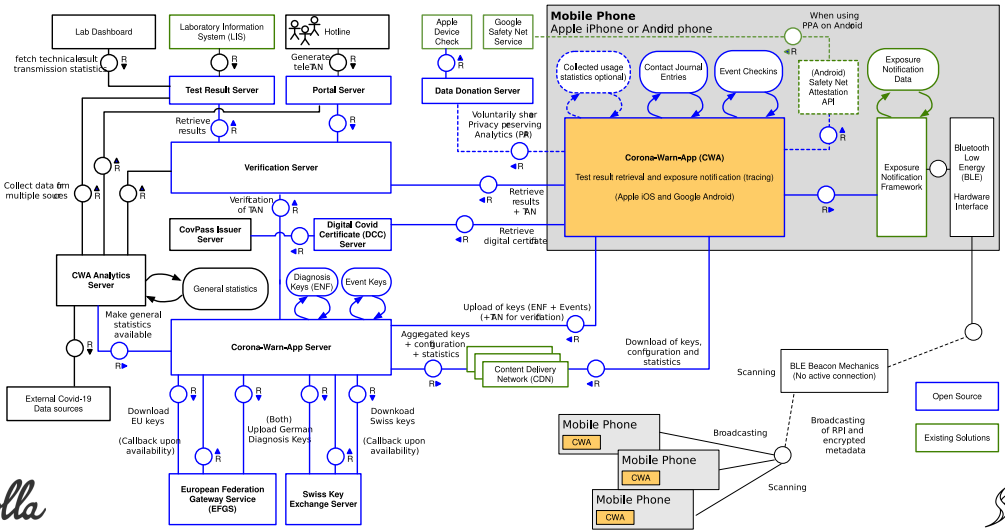
WORKING WITH GOOGLE AND APPLE

A great job with the design, specs, API but no collaboration

1. No direct interaction
2. Specs provided early
3. The promised test data never materialised
4. Relevant code not released until too late
5. Nevertheless, the specs were good enough to implement

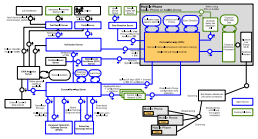
1. This was as you might expect: great at documentation, not great at interaction.
2. The app reference design released early, 4 May 2020 [5].
3. But the *internals* needed for implementation released later, 27 July 2020 [6].

WORKING WITH SAP



jolla

SAILFISH OS



1. The CWA infrastructure contained many app-facing moving parts
   1.1 **Download server** (CWA Server) for downloading risk configurations and daily beacon database
   1.2 **Verification Server** for matching TANs to diagnoses
   1.3 **Upload Server** (CWA Server but actually a different server) for uploading beacon keys
2. Deploying everything was impractical, but SAP released reference implementations.
3. The reference *download* server was a bit broken, but otherwise good.
4. The reference *verification* and *upload* servers were minimal.
5. We fixed the reference implementations and deployed them to AWS.

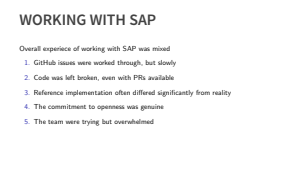
WORKING WITH SAP

Overall experiece of working with SAP was mixed

1. GitHub issues were worked through, but slowly
2. Code was left broken, even with PRs available
3. Reference implementation often differed significantly from reality
4. The commitment to openness was genuine
5. The team were trying but overwhelmed

Covid Exposure Notification Out in the Open

Working with SAP



1. SAP and Deutsche Telekom developed Germany's Covid Warn App [7].
2. Lots of code, lots of documentation, even an evaluation against CCC requirements [8].
3. One of the earliest and most open in Europe.

REFLECTIONS

1. A huge challenge for governments and organisations
2. Need for speed, effectiveness and openness
3. Google, Apple and the CWA team *got* this in theory
4. Scope for improvement in practice
5. Information flowed outwards, little flowed inwards
6. More generally, lack of appreciation of open source development model effort

jolla

SAILFISH OS

REFLECTIONS
1. A huge challenge for governments and organisations
2. Need for speed, effectiveness and openness
3. Google, Apple and the CWA team got this in theory
4. Scope for improvement in practice
5. Information flowed outwards, little flowed inwards
6. More generally, lack of appreciation of open source development model effort

1. It's important to put this in context: there was a *lot* of pressure
2. There were many *competing* requirements
3. Not all governments understood the need for openness
4. Nevertheless it's good to try to learn from the experiences
5. With SAP in particular, I was impressed by their intentions, although there was little inward info flow, even when it could have benefited them
6. Problem: how to know what inward info will be of benefit; this required effort
7. Overall, given the organisations had no duty towards me as an independent developer, I was impressed with the commitment to privacy and openness

FURTHER INFO

Sailfish OS	`https://sailfishos.org`
Contrac	`https://github.com/llewelld/harbour-contrac`
GAEN spec	`https://www.google.com/covid19/exposurenotifications`
Covid Warn App	`https://github.com/corona-warn-app`
Linux on Mobile	Building K, upstairs

jolla

SAILFISH OS

Covid Exposure Notification Out in the Open

Further info

FURTHER INFO

Sailfish OS	https://sailfishos.org
Contrac	https://github.com/llewelld/harbour-contrac
GAEN spec	https://www.google.com/covid19/exposurenotifications
Covid Warn App	https://github.com/corona-warn-app
Linux on Mobile	Building K, upstairs

[1] Google, "Exposure notifications specification." https://www.google.com/covid19/exposurenotifications, 10 April 2020.

[2] Johns Hopkins Center for Health Security, "Review of mobile application technology to enhance contact tracing capacity for covid-19," 8 April 2020.

[3] D. Llewellyn-Jones, "libcontrac." https://github.com/llewelld/libcontrac, 18 April 2020.

[4] D. Llewellyn-Jones and O. Roesler, "Contrac." https://github.com/llewelld/harbour-contrac, 28 April 2020.

[5] Google, "Exposure notification app reference design." https://github.com/google/exposure-notifications-android, 4 May 2020.

[6] Google, "Exposure notifications internals." https://github.com/google/exposure-notifications-internals, 27 July 2020.

[7] SAP and Deutsche Telekom, "Covid warn app." https://github.com/corona-warn-app, 12 May 2020.

[8] SAP and Deutsche Telekom, "Criteria for the evaluation of contact tracing apps." https://github.com/corona-warn-app/cwa-documentation/blob/main/pruefsteine.md, 2 June 2020.