

Corona-Warn-App

Behind the scenes: Invisible, yet important

Thomas Klingbeil, SAP SE
December 30, 2020

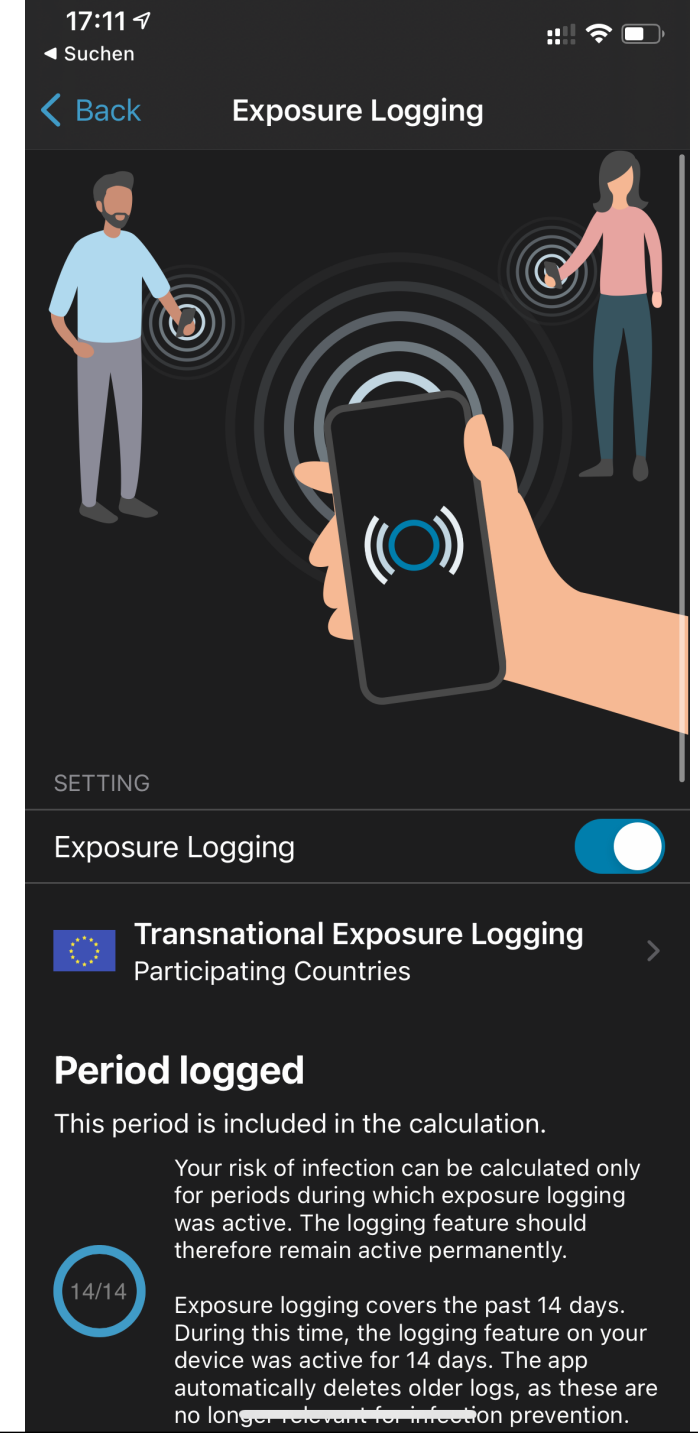
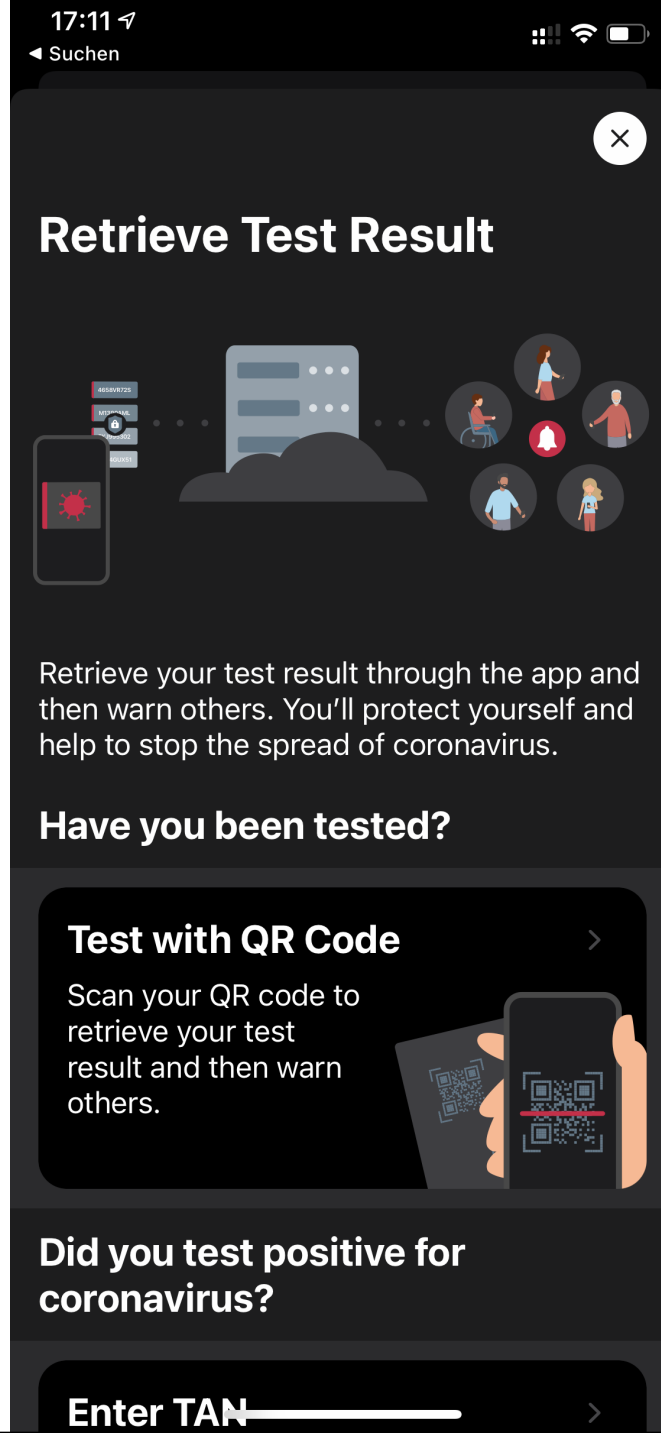
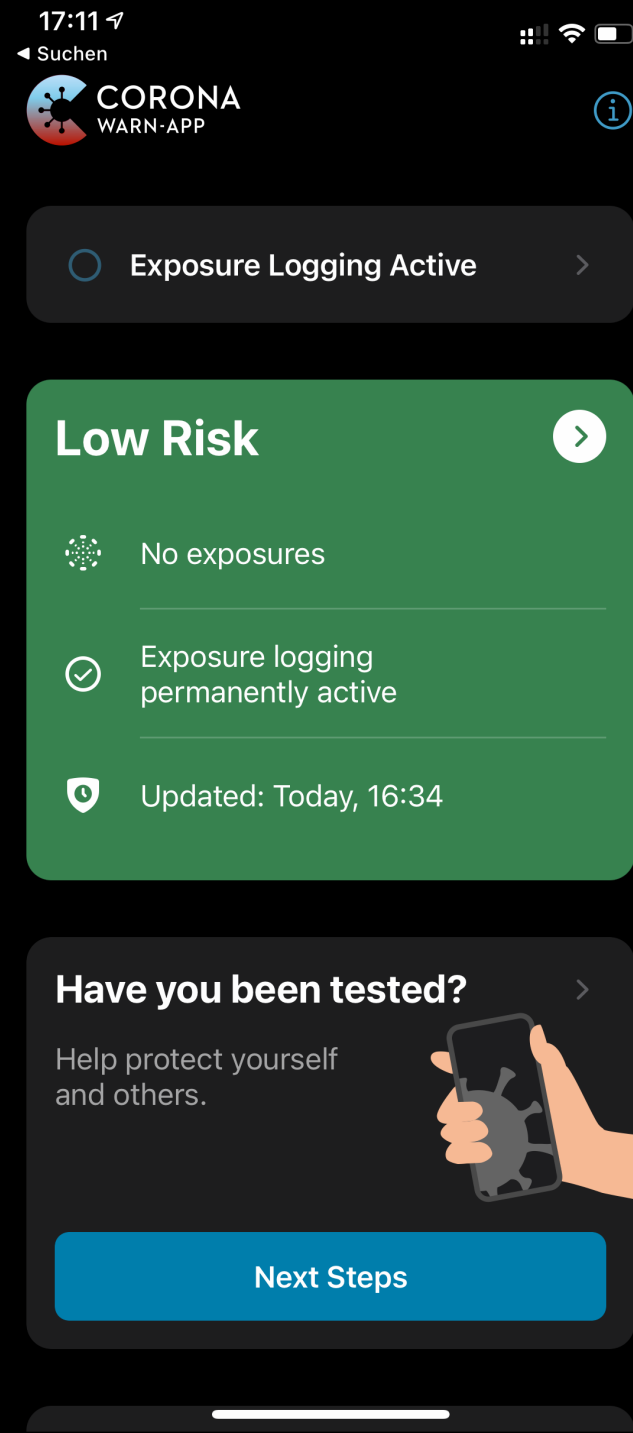
PUBLIC

Agenda

- Introduction to the app and its **architecture**
- **Communication** with the backend
- Risk **calculation**

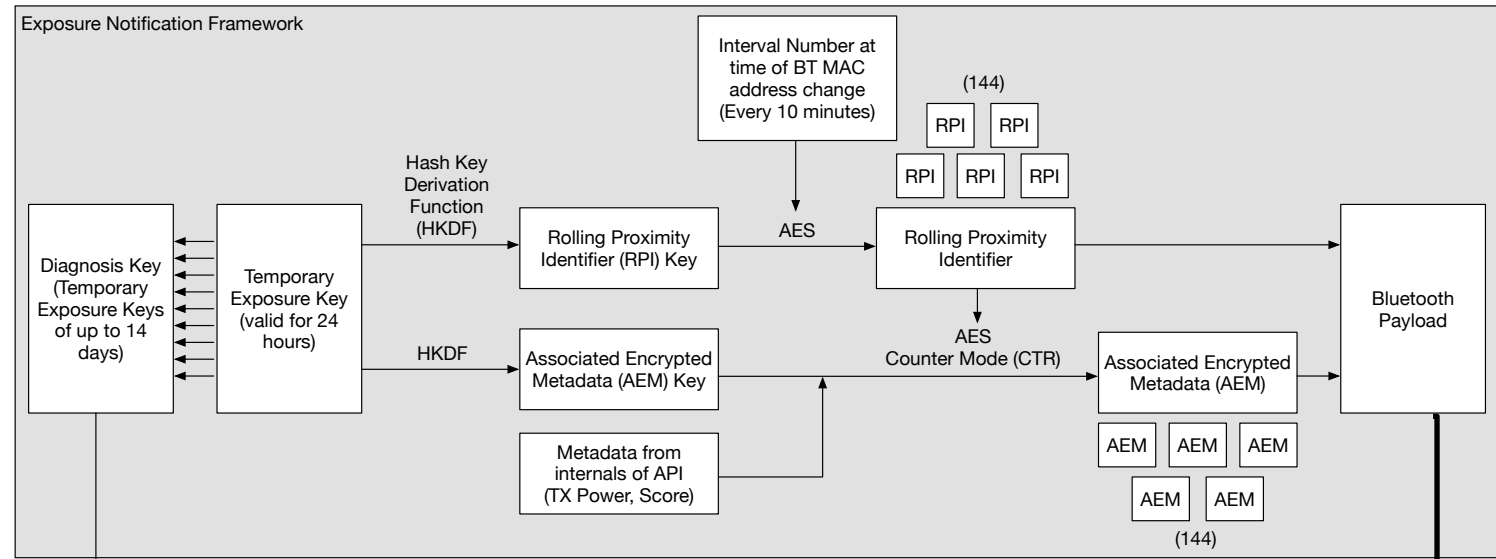
Introduction:

Corona-Warn-App? What's that?



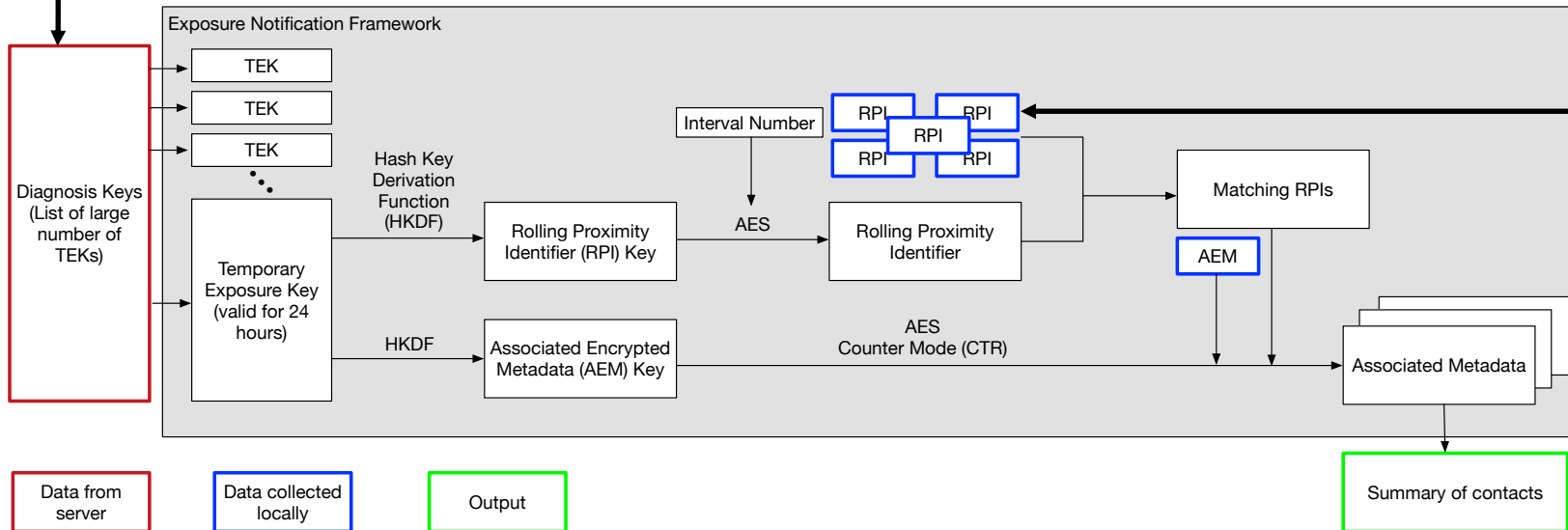
Exposure Notification

Terminology



through server

Diagnosis Key for upload



BLE Beacon mechanics

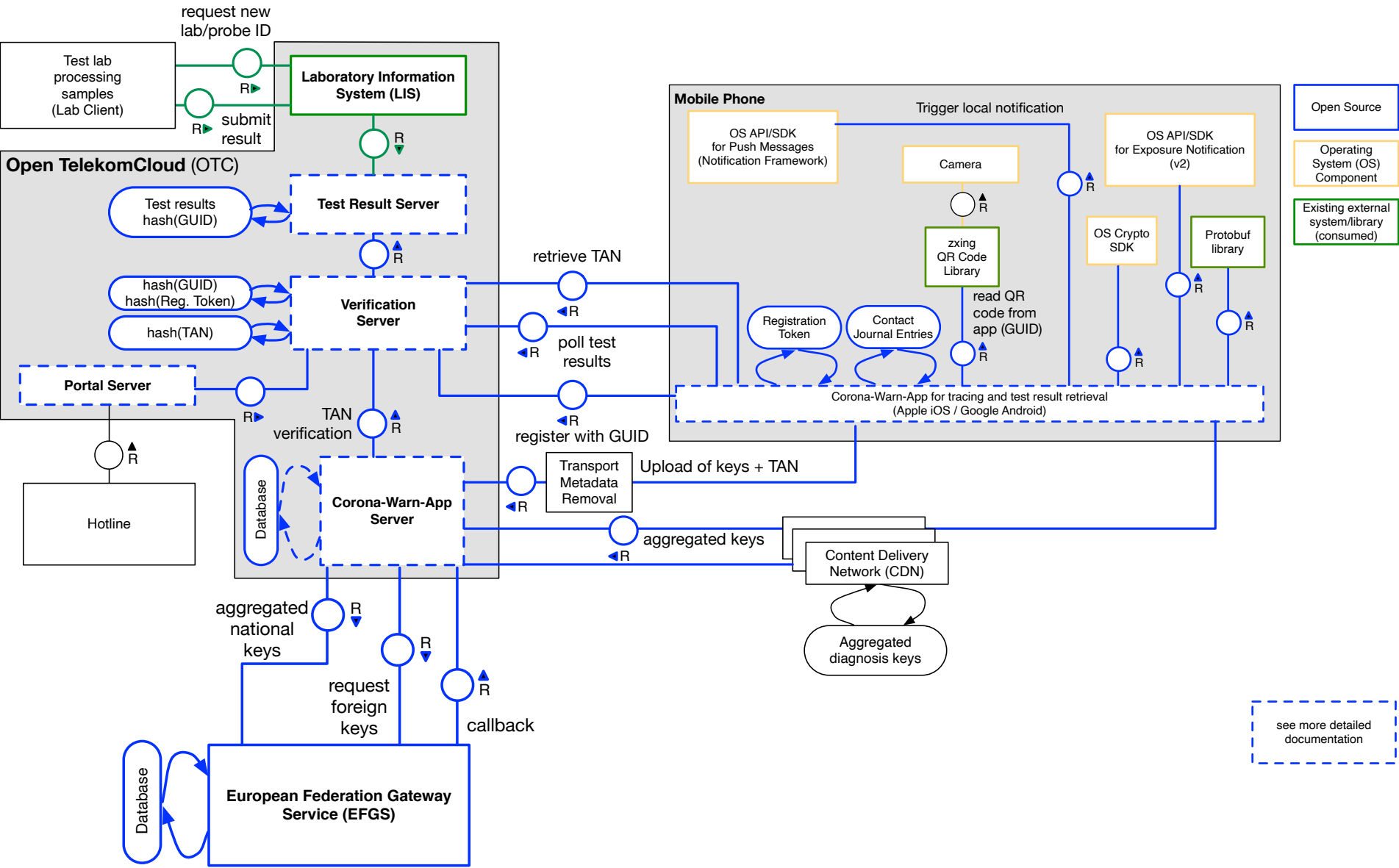
Data from server

Data collected locally

Output

Summary of contacts

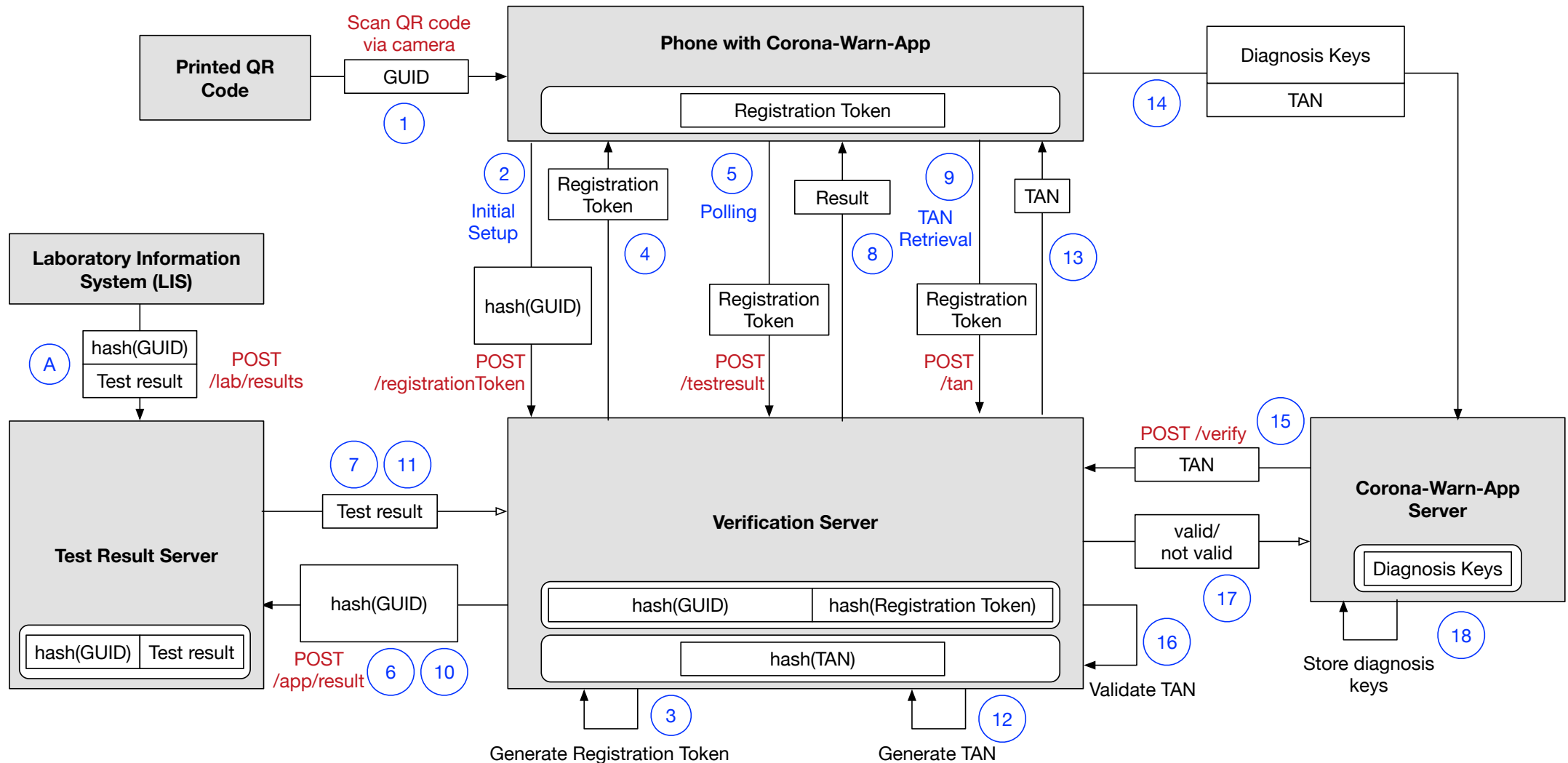
Architecture Overview



Communication with the backend

What happens if someone is listening?

Data flow for test result retrieval using QR codes



What could be found out by **observing the network traffic**

Assumption: The content of the messages is secure, only connections and size of transfer are observable

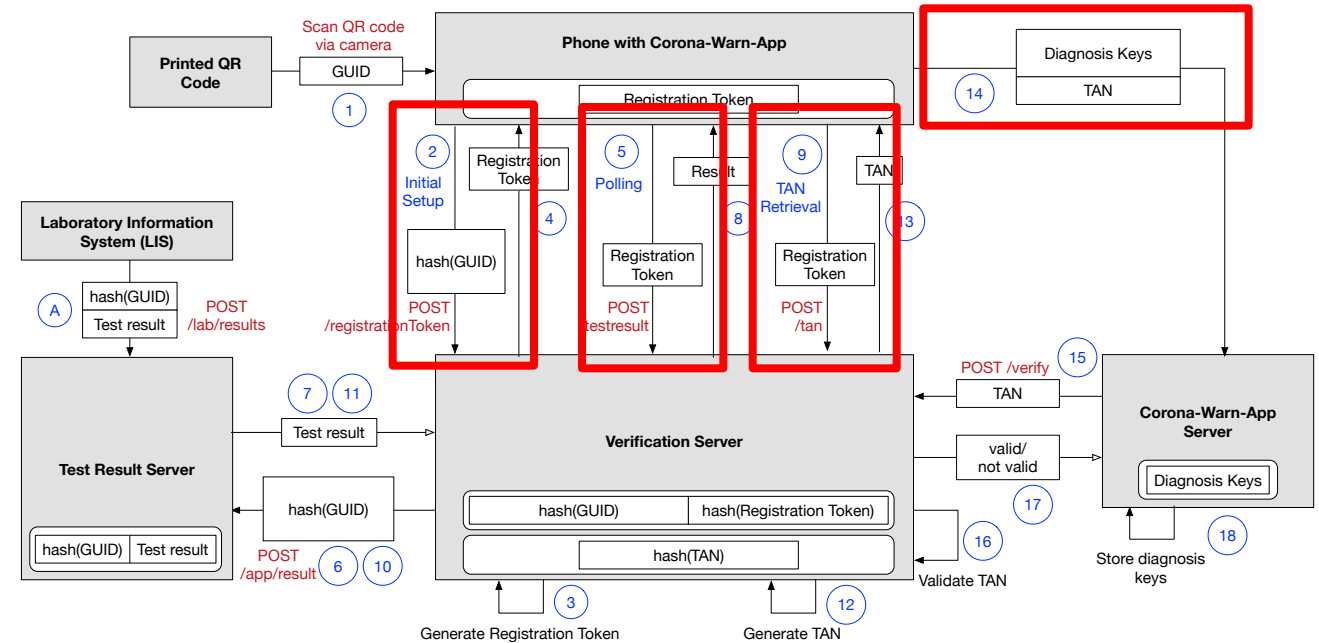
(2) The person has been tested

(5) The person has been tested and still has not received the test result yet

(9) The person has been tested positive

(14) The person has been tested positive and is in the process of sharing keys

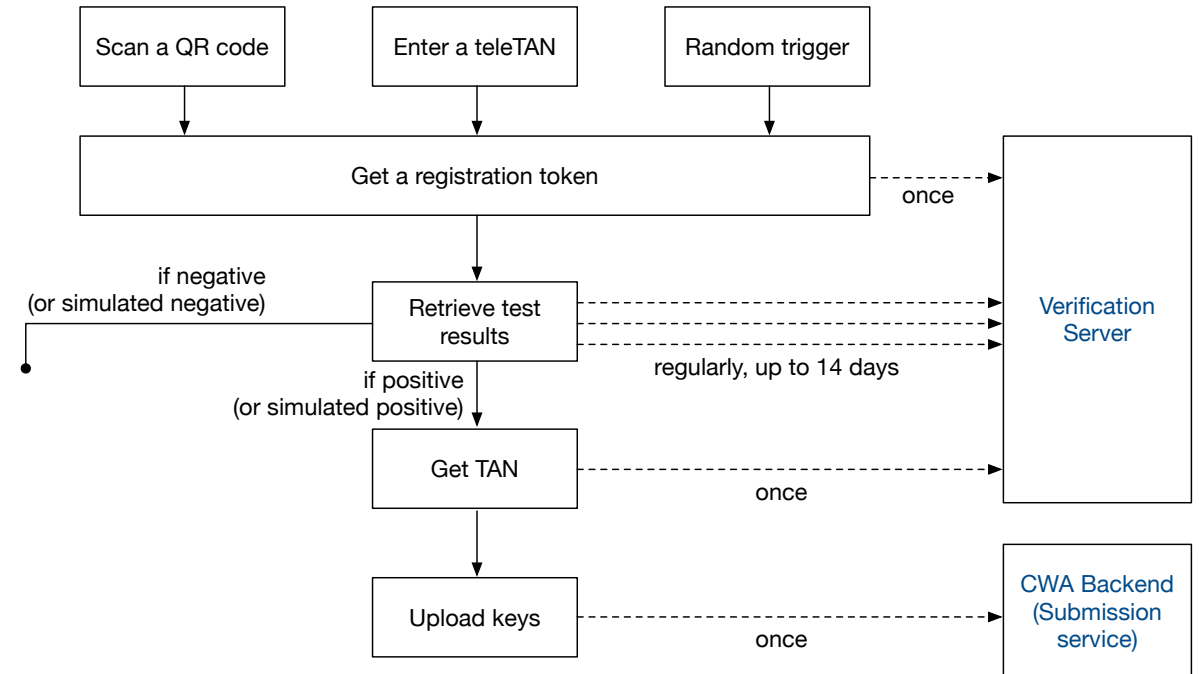
+ Keys could be related to an origin address



We need to establish plausible deniability

How to **prevent** extraction of information through **observation**

- Apps simulate backend traffic by sending „fake“ or „dummy“ requests
 - Either triggered by a real event or randomly
 - Apply padding to requests
- Special header field informs backend to react accordingly
 - Do not interact with underlying database
 - Delay response according to real behaviour
 - Apply padding, so size does not give away content of response
- No extra cost for mobile data → zero rating



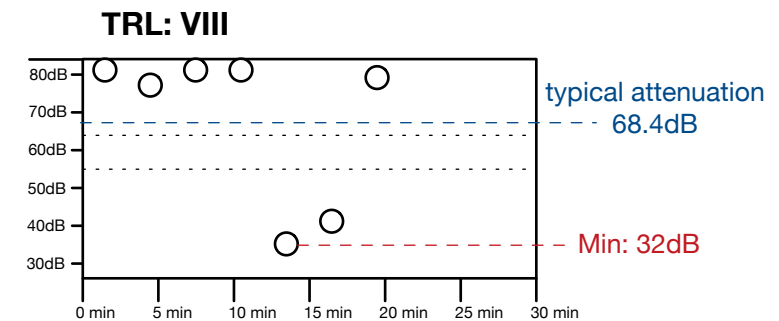
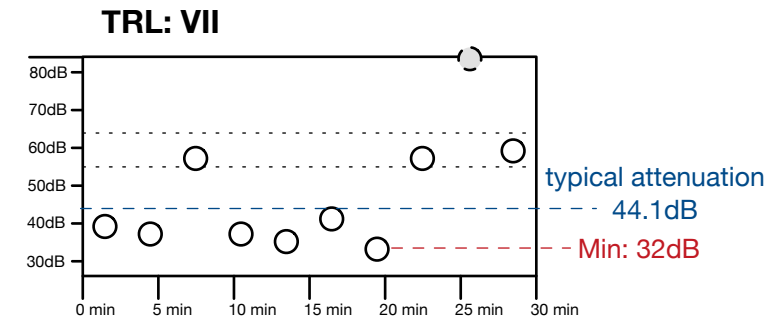
How to **prevent** extraction of information through **metadata**

- When uploading keys, the HTTP(S) request from the mobile phone carries metadata
 - Source IP address
 - User agent (Operating System, possibly also OS version)
- Before the request reaches the backend server, the metadata is removed
 - only the content is forwarded to the backend service

Risk calculation

How the risk is being calculated

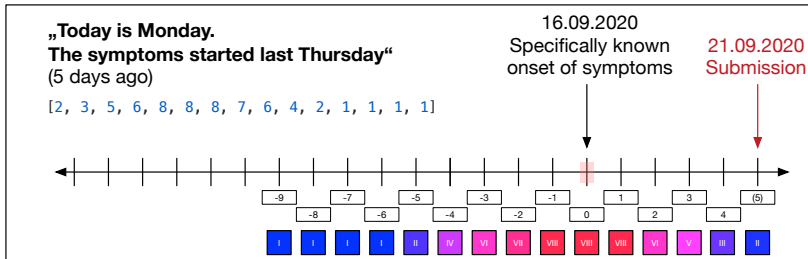
- Information about encounters (calculated at device receiving the RPI), provided in 30 minute exposure windows
 - number of scan instances (=duration of the encounter)
 - signal attenuation (minimum/average per scan instance)
 - reported TX power – RX = attenuation
 - low attenuation → close
 - higher attenuation → farther away
- Information provided within the uploaded keys
 - Transmission Risk Level (= infectiousness)



Transmission Risk Level - based on symptom status

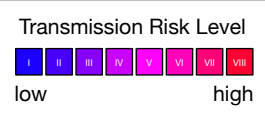
Deriving the Transmission Risk Level from
Days since Onset of Symptoms (specific date is known)

Value range (EFGS): -14 to 21



Transmission Risk Level - based on symptom status

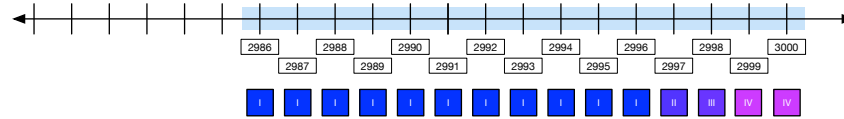
Deriving the Transmission Risk Level from
Days since Onset of Symptoms (explicitly no symptoms)
—> technically „days since submission“
Value range (EFGS): 2986 to 3000



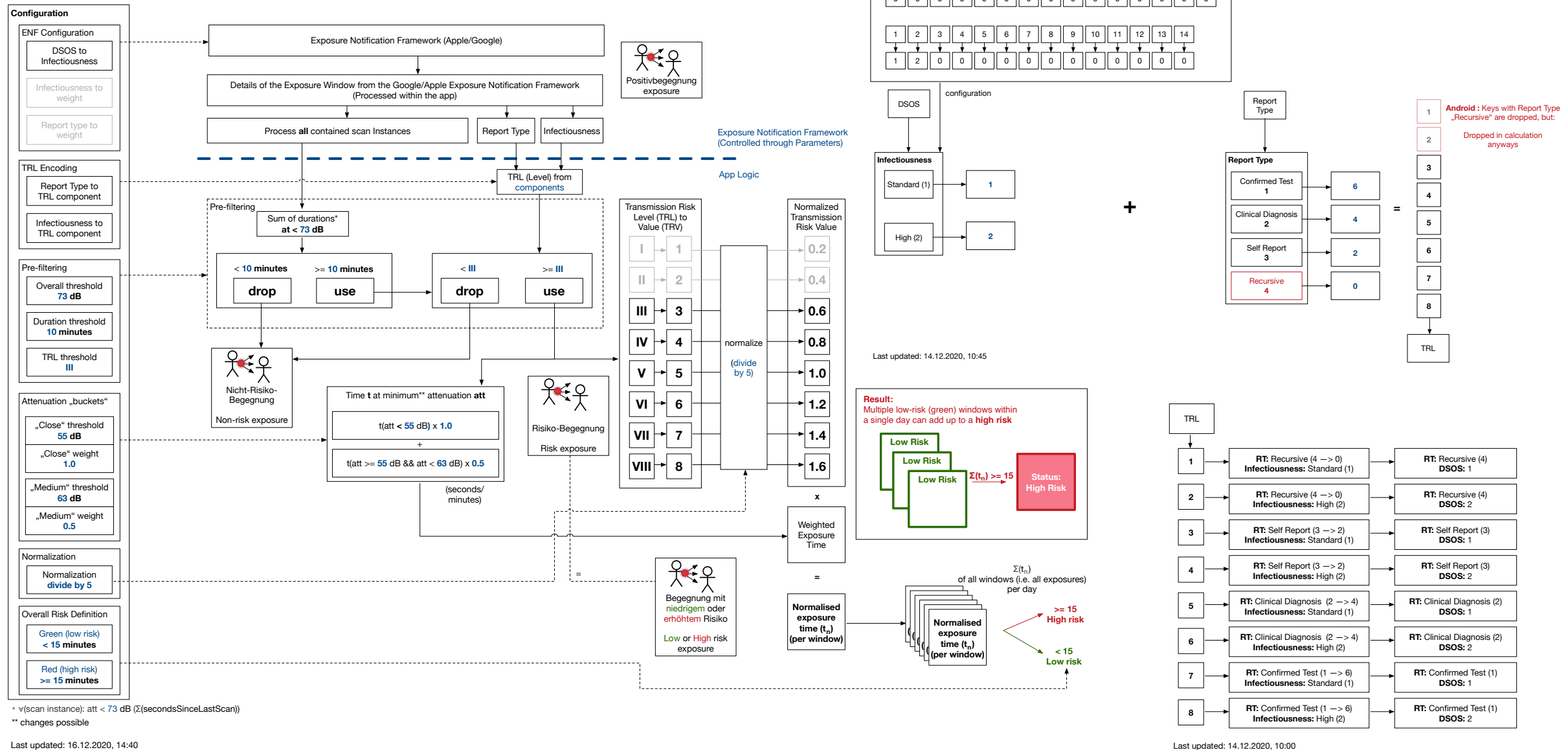
„Today is Monday. I just received a positive test result,
but I never had symptoms.“

[4, 4, 3, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1]

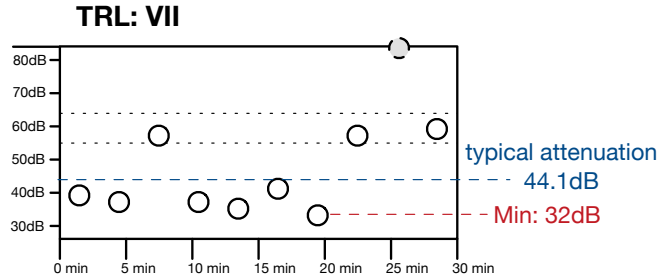
21.09.2020
Submission



Risk calculation



High or low risk for those windows? Red or Green?



- Pre-Filtering
 - At least 10 minutes <73dB? Yes.
 - At least TRL III? Yes.

- Calculation:
 - 18 minutes at low attenuation → 18.0 minutes
 - 9 minutes at medium attenuation → 4.5 minutes
 - TRL VII → $(=7/5) \rightarrow \times 1.4$
 - $(18.0+4.5) \times 1.4 = 31.5$ minutes → **red!**

- Pre-Filtering
 - At least 10 minutes <73dB? No.
→ Dropped

- Pre-Filtering
 - At least 10 minutes <73dB? Yes.
 - At least TRL III? Yes.

- Calculation:
 - 6 minutes at low attenuation → 6.0 minutes
 - 0 minutes at medium attenuation → 0.0 minutes
 - TRL VIII → $(=8/5) \rightarrow \times 1.6$
 - $(6.0+0.0) \times 1.6 = 9.6$ minutes → **green.**

Thank you!

Learn more at

www.coronawarn.app

<https://github.com/corona-warn-app>

Follow us



www.sap.com/contactsap

© 2019 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.

SAP folgen auf



www.sap.com/germany/contactsap

© 2019 SAP SE oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP SE oder ein SAP-Konzernunternehmen nicht gestattet.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die von SAP SE oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der SAP SE oder einem SAP-Konzernunternehmen bereitgestellt und dienen ausschließlich zu Informationszwecken. Die SAP SE oder ihre Konzernunternehmen übernehmen keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die SAP SE oder ein SAP-Konzernunternehmen steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

Insbesondere sind die SAP SE oder ihre Konzernunternehmen in keiner Weise verpflichtet, in dieser Publikation oder einer zugehörigen Präsentation dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen. Diese Publikation oder eine zugehörige Präsentation, die Strategie und etwaige künftige Entwicklungen, Produkte und/oder Plattformen der SAP SE oder ihrer Konzernunternehmen können von der SAP SE oder ihren Konzernunternehmen jederzeit und ohne Angabe von Gründen unangekündigt geändert werden. Die in dieser Publikation enthaltenen Informationen stellen keine Zusage, kein Versprechen und keine rechtliche Verpflichtung zur Lieferung von Material, Code oder Funktionen dar. Sämtliche vorausschauenden Aussagen unterliegen unterschiedlichen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können. Dem Leser wird empfohlen, diesen vorausschauenden Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.

SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP SE (oder von einem SAP-Konzernunternehmen) in Deutschland und verschiedenen anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.

Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite www.sap.com/corporate/de/legal/copyright.html.