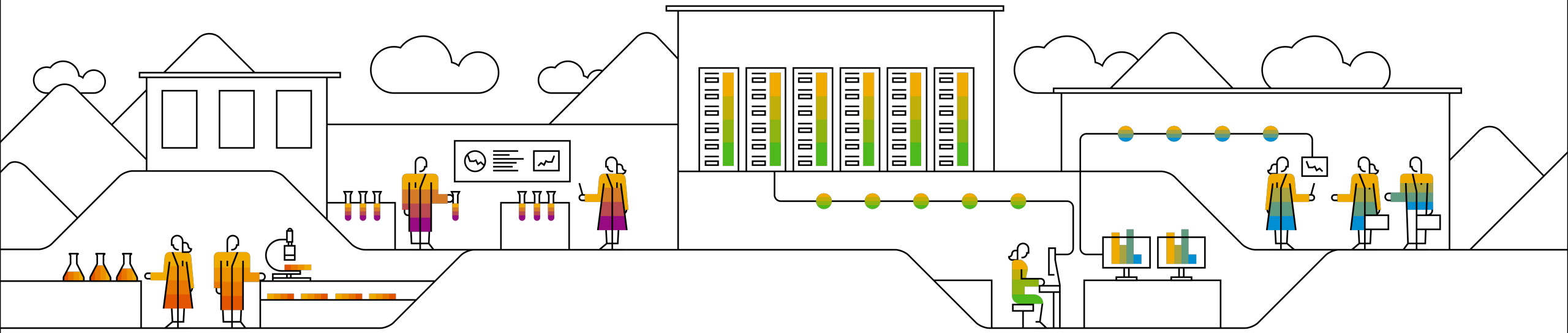


Corona-Warn-App

Behind the scenes: Invisible, yet important

Thomas Klingbeil, SAP SE
December 30, 2020

PUBLIC

THE BEST RUN SAP

Agenda

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

Introduction:

Corona-Warn-App? What‘s that?

17:11
◀ Suchen

CORONA WARN-APP

Exposure Logging Active

Low Risk

No exposures

Exposure logging permanently active

Updated: Today, 16:34

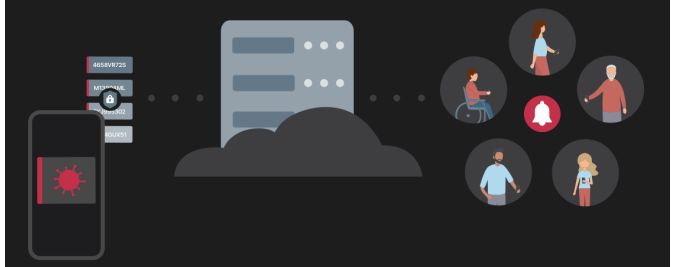
Have you been tested?

Help protect yourself and others.

Next Steps

17:11
◀ Suchen

Retrieve Test Result



Retrieve your test result through the app and then warn others. You'll protect yourself and help to stop the spread of coronavirus.

Have you been tested?

Test with QR Code

Scan your QR code to retrieve your test result and then warn others.

Did you test positive for coronavirus?

Enter TAN

17:11
◀ Suchen

Back

Exposure Logging

SETTING

Exposure Logging

Transnational Exposure Logging
Participating Countries

Period logged

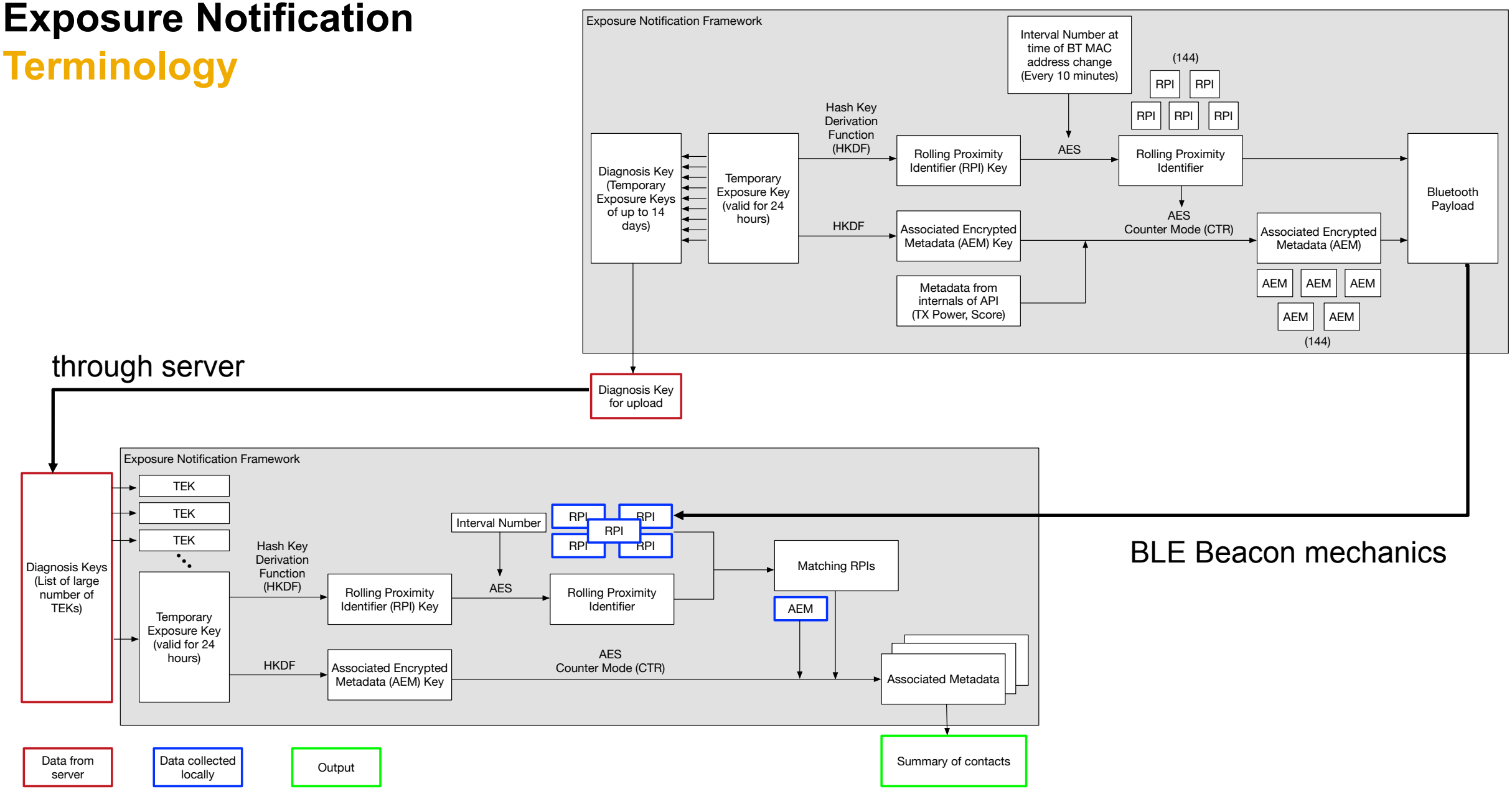
This period is included in the calculation.

14/14

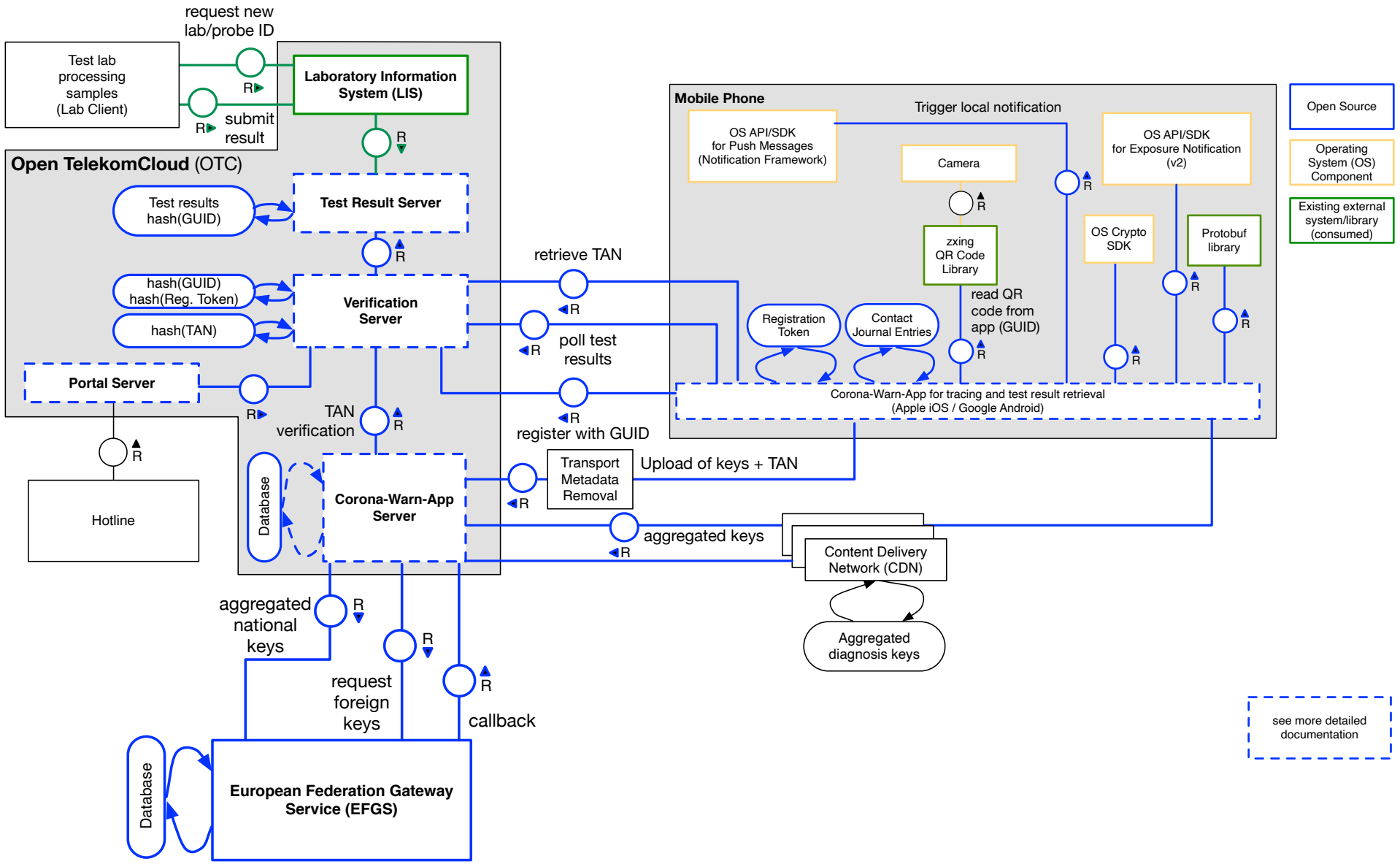
Your risk of infection can be calculated only for periods during which exposure logging was active. The logging feature should therefore remain active permanently.

Exposure logging covers the past 14 days. During this time, the logging feature on your device was active for 14 days. The app automatically deletes older logs, as these are no longer relevant for infection prevention.

Exposure Notification
Terminology



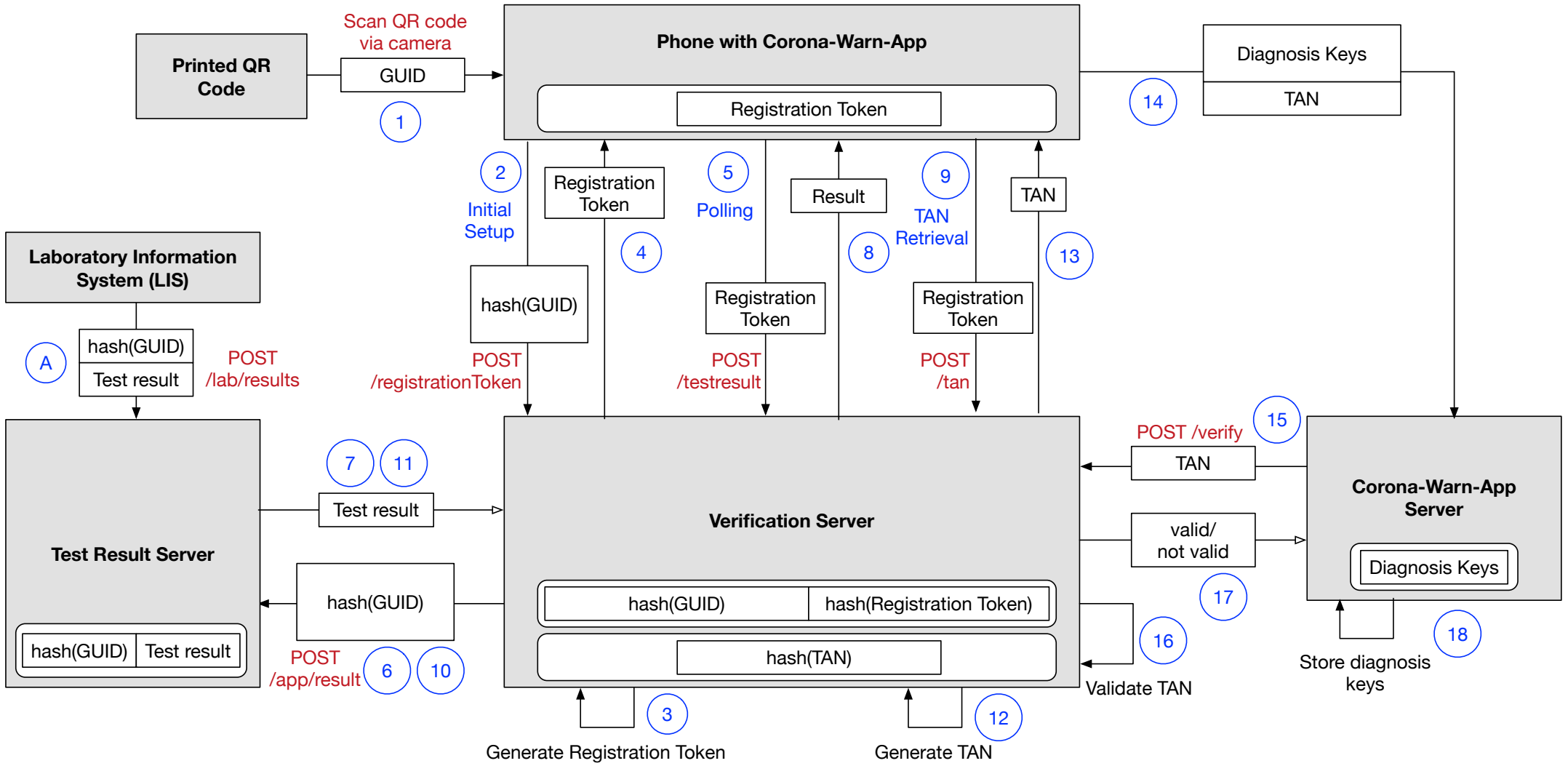
Architecture Overview



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

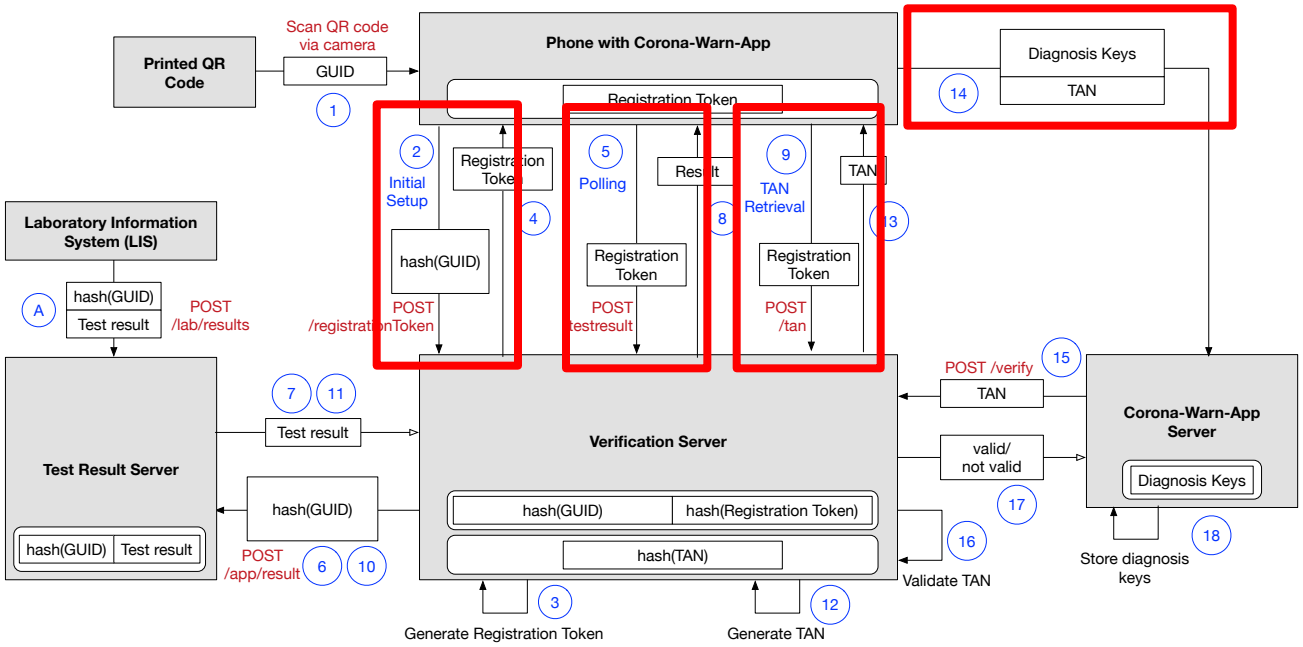
(2) The person has been tested

(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

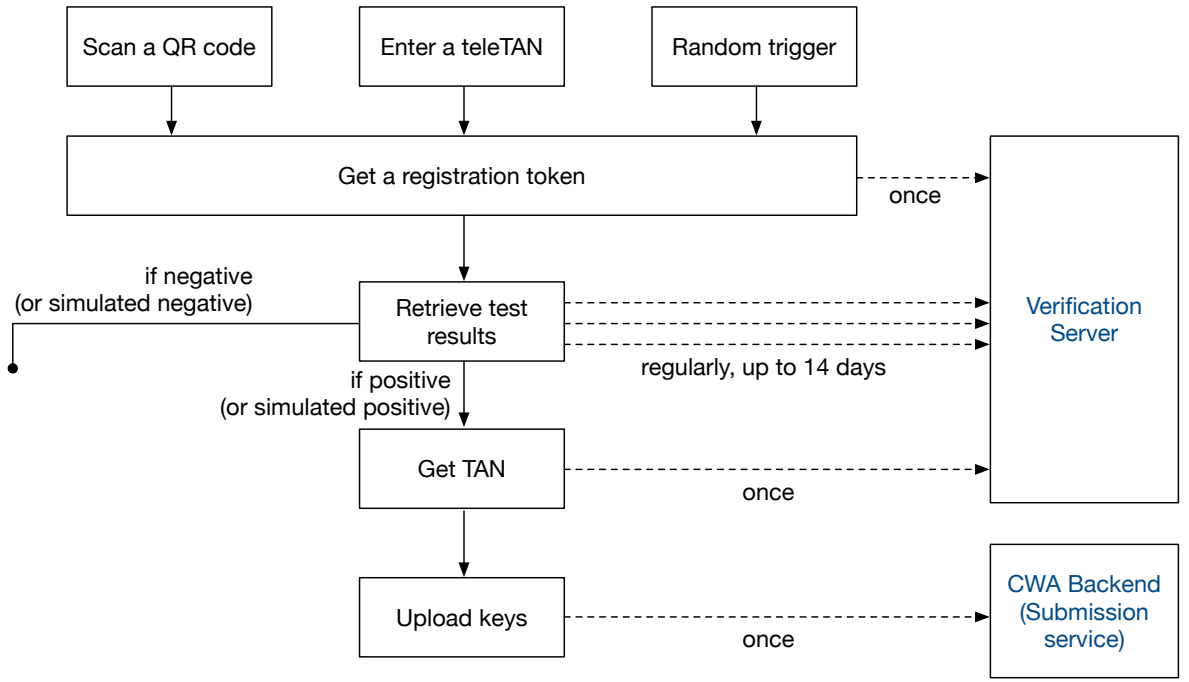
+ Keys could be related to an origin address



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

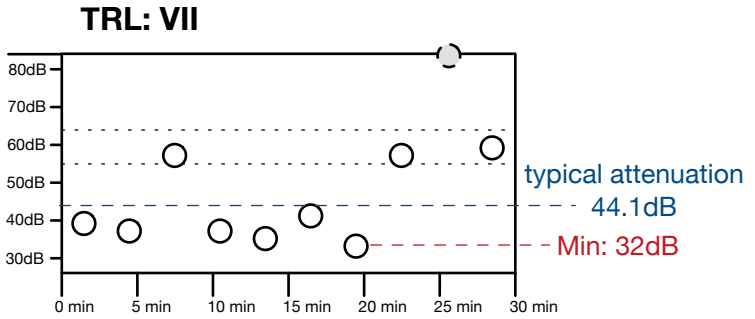
- When uploading keys, the HTTP(S) request from the mobile phone carries metadata
  - Source IP address
  - User agent (Operating System, possibly also OS version)

- Before the request reaches the backend server, the metadata is removed
  - only the content is forwarded to the backend service

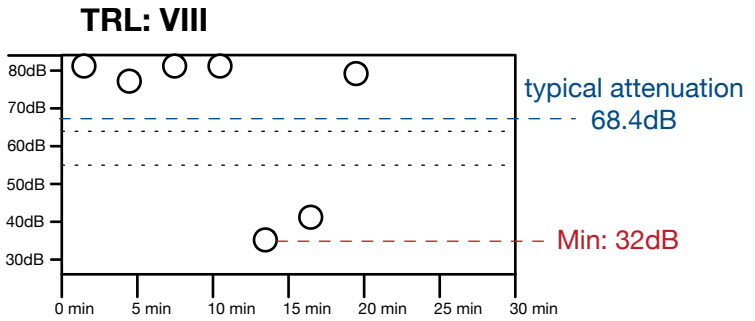
Risk calculation

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



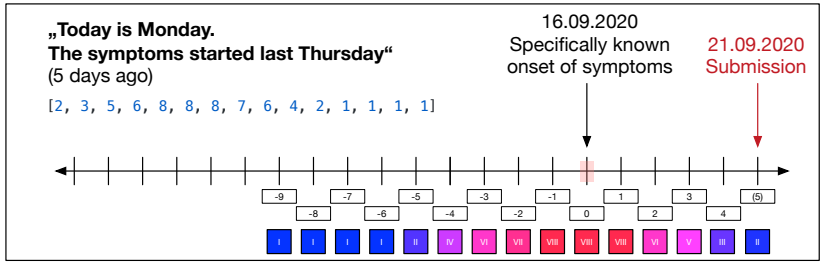
- Information provided within the uploaded keys
  - Transmission Risk Level (= infectiousness)



Transmission Risk Level - based on symptom status

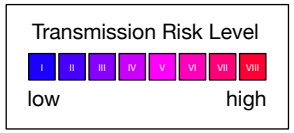
Deriving the Transmission Risk Level from
Days since Onset of Symptoms (specific date is known)

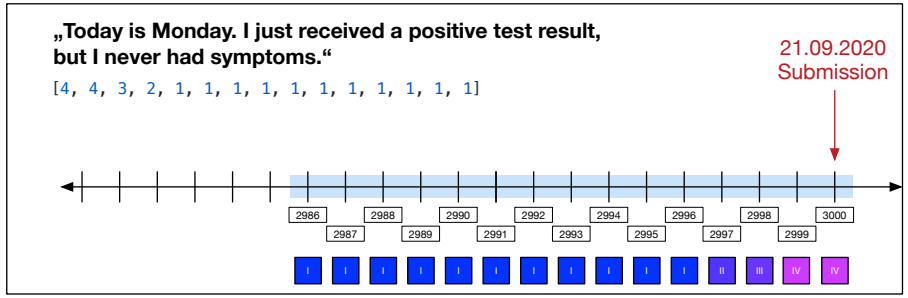
Value range (EFGS): -14 to 21



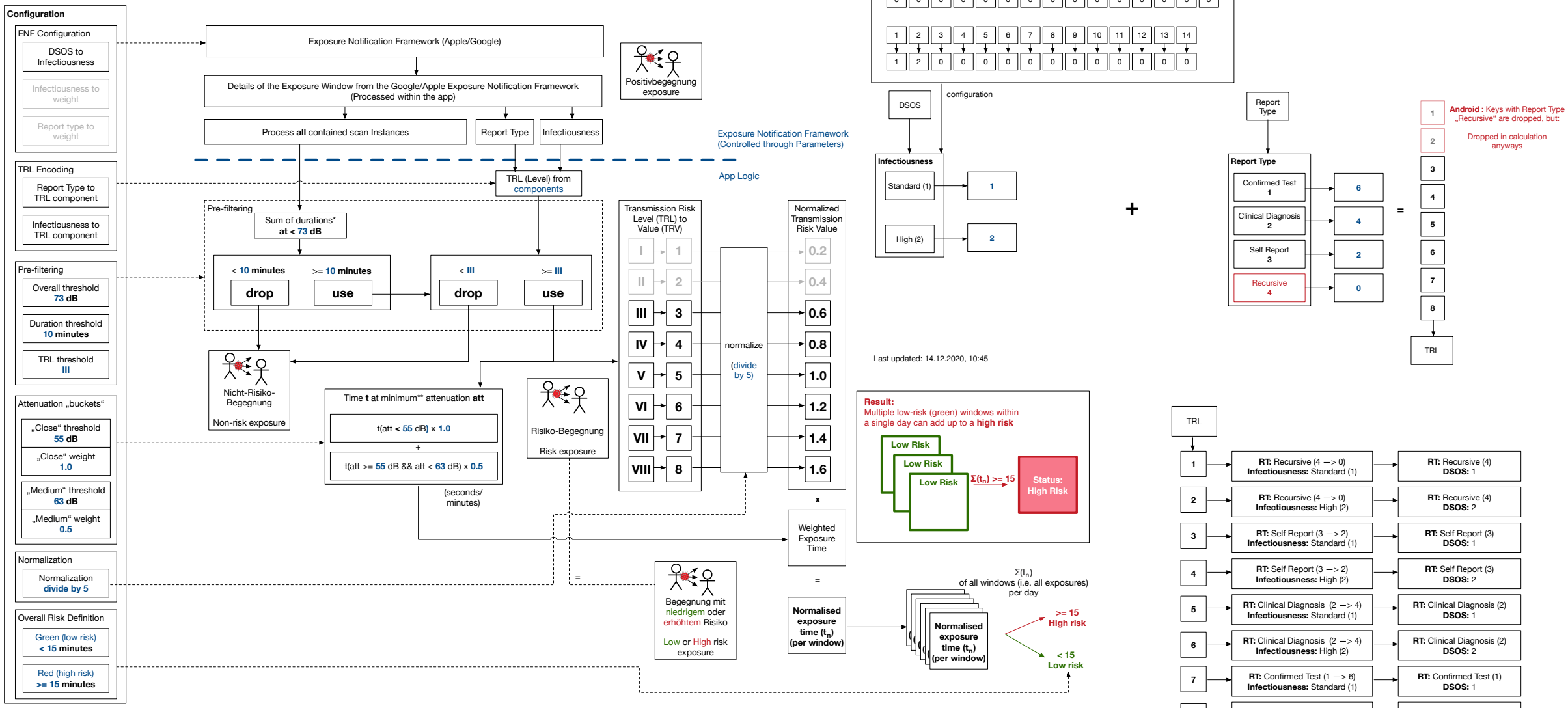
Transmission Risk Level - based on symptom status

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

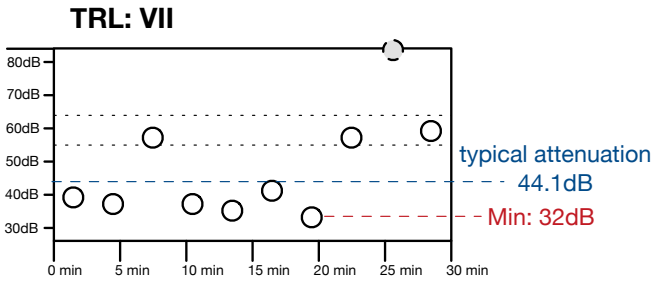




Risk calculation



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) → x1.4
  - (18.0+4.5) x 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) → x1.6
  - (6.0+0.0) x 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

THE BEST RUN SAP®

SAP folgen auf

www.sap.com/germany/contactsap

THE BEST RUN SAP®