Corona-Warn-App

Behind the scenes: Invisible, yet important

Thomas Klingbeil, SAP SE
December 30, 2020

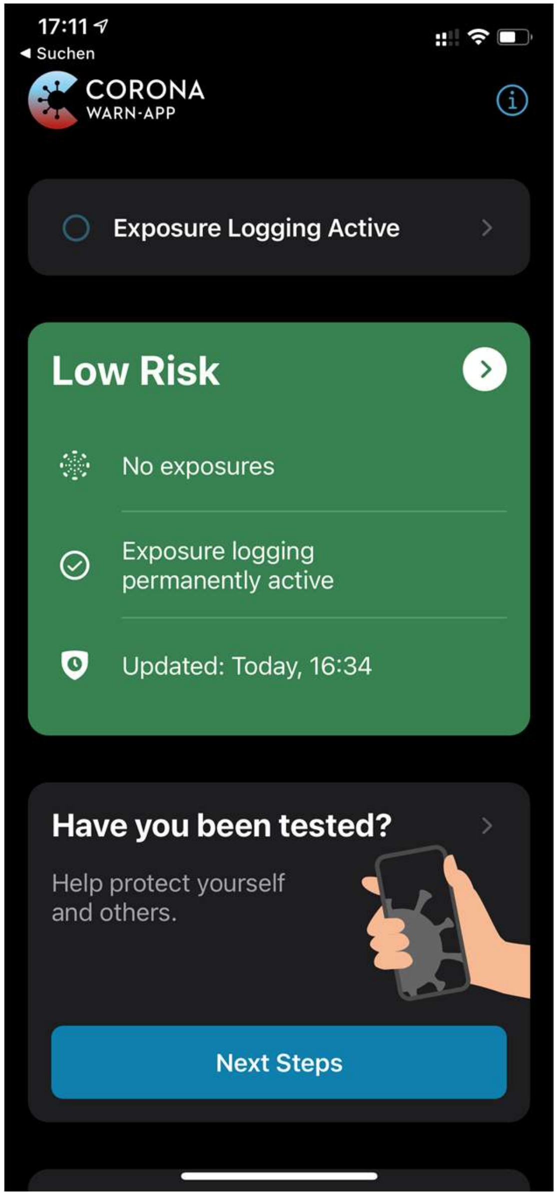
PUBLIC

Agenda

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

Introduction:

Corona-Warn-App? What‘s that?



Exposure Logging Active

Low Risk

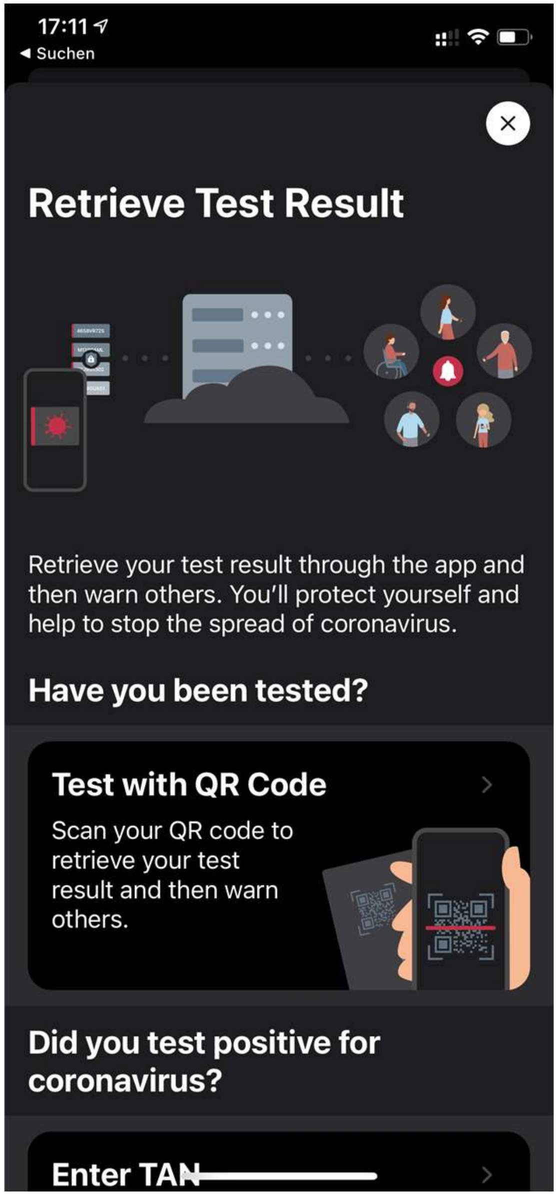
No exposures

Exposure logging permanently active

Updated: Today, 16:34

Have you been tested?

Help protect yourself and others.



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.

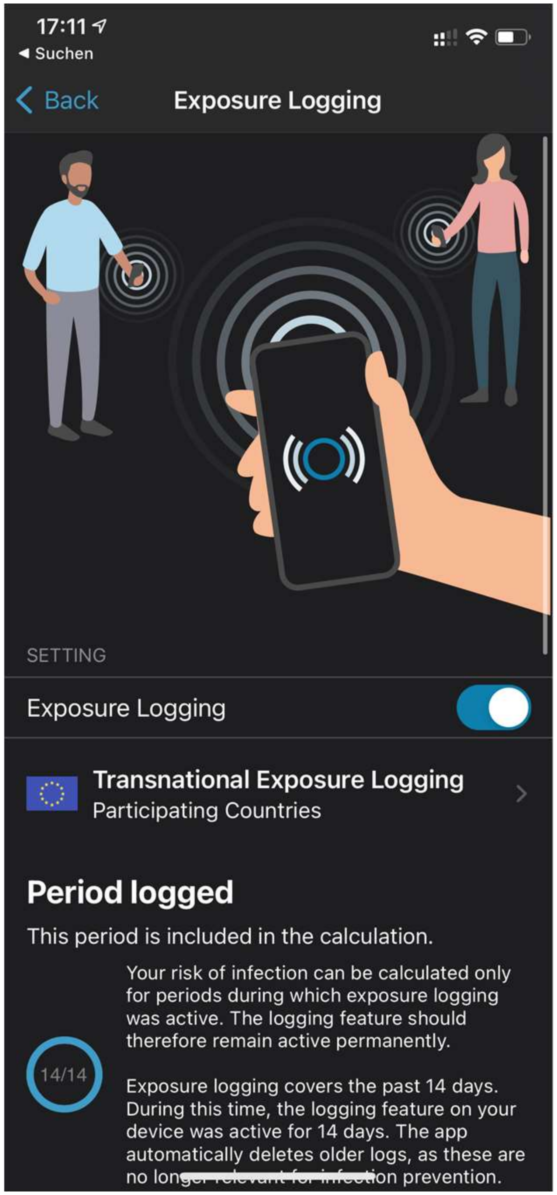
Have you been tested?

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



Exposure Logging

SETTING

Exposure Logging ●

Transnational Exposure Logging
Participating Countries

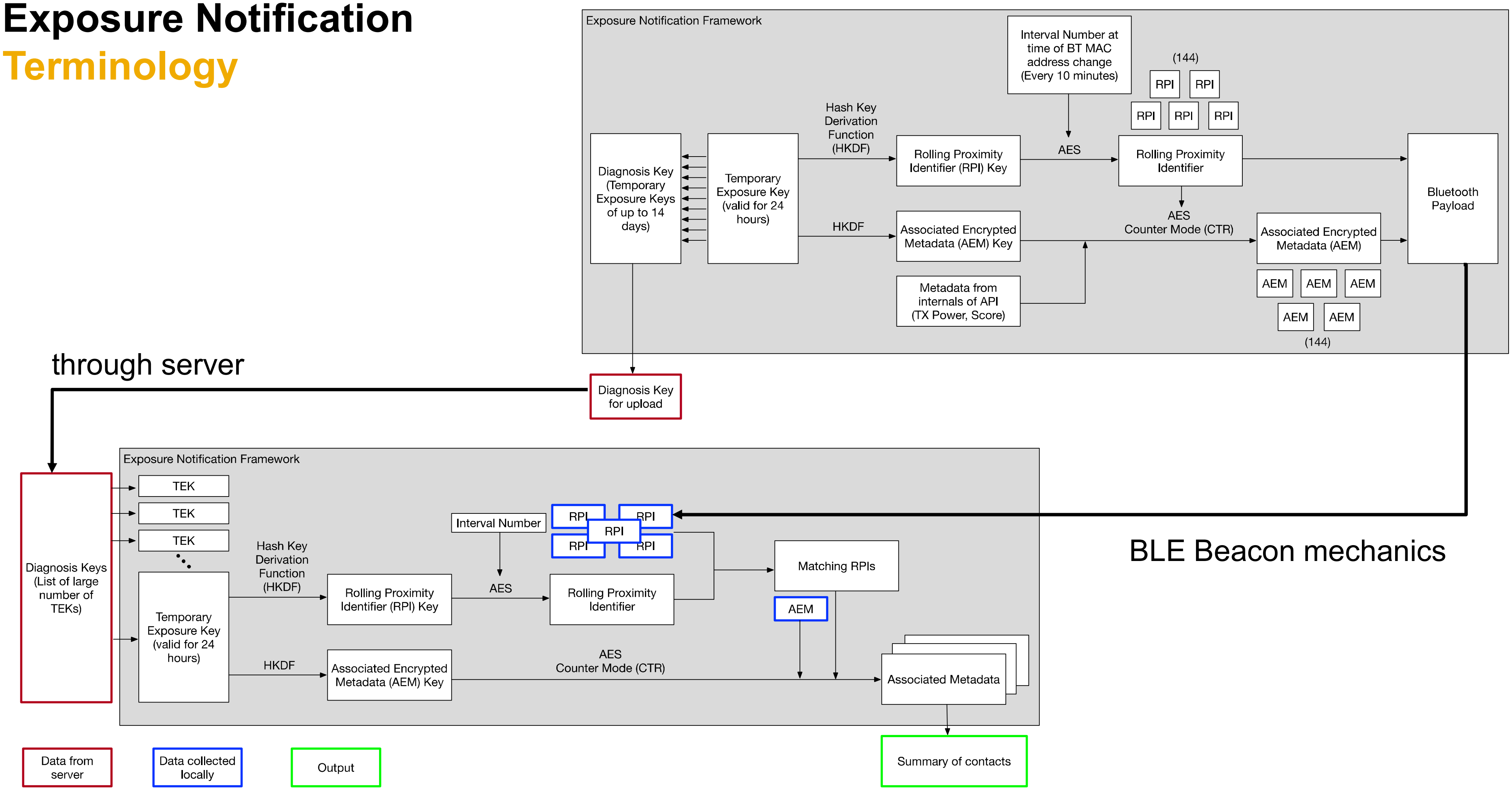
Period logged

This period is included in the calculation.

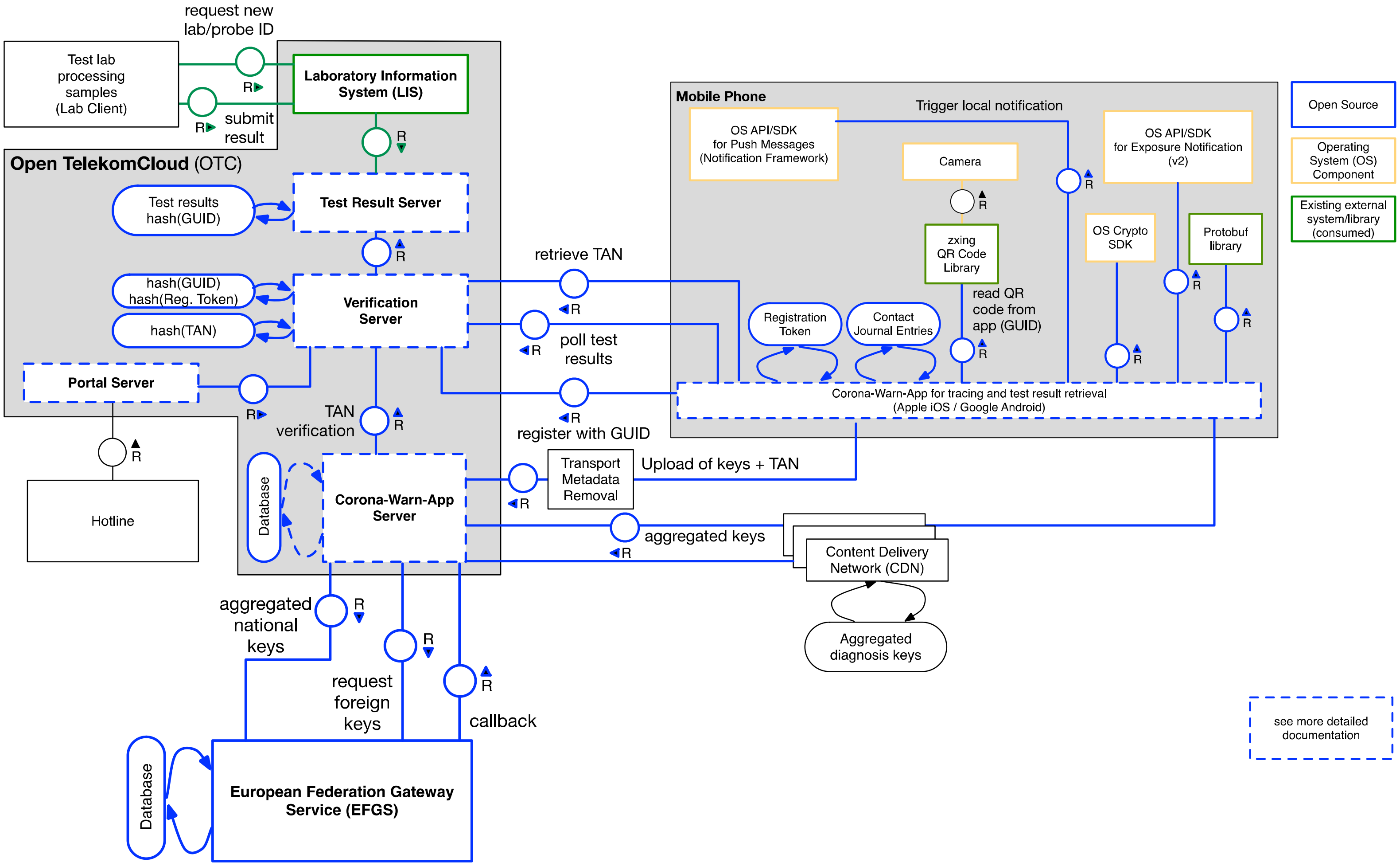
Your risk of infection can be calculated only for periods during which exposure logging was active. The logging feature should therefore remain active permanently.

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


Exposure Notification Framework
Interval Number at time of BT MAC address change (Every 10 minutes)
(144)
RPI
RPI
RPI
RPI
RPI
Hash Key Derivation Function (HKDF)
AES
Diagnosis Key (Temporary Exposure Keys of up to 14 days)
Temporary Exposure Key (valid for 24 hours)
Rolling Proximity Identifier (RPI) Key
Rolling Proximity Identifier
Bluetooth Payload
HKDF
AES Counter Mode (CTR)
Associated Encrypted Metadata (AEM) Key
Associated Encrypted Metadata (AEM)
Metadata from internals of API (TX Power, Score)
AEM
AEM
AEM
AEM
AEM
(144)
through server
Diagnosis Key for upload
Exposure Notification Framework
TEK
TEK
TEK
Diagnosis Keys (List of large number of TEKs)
Temporary Exposure Key (valid for 24 hours)
Hash Key Derivation Function (HKDF)
Rolling Proximity Identifier (RPI) Key
Interval Number
AES
RPI
RPI
RPI
RPI
RPI
Rolling Proximity Identifier
Matching RPIs
AEM
BLE Beacon mechanics
HKDF
Associated Encrypted Metadata (AEM) Key
AES Counter Mode (CTR)
Associated Metadata
Summary of contacts
Data from server
Data collected locally
Output

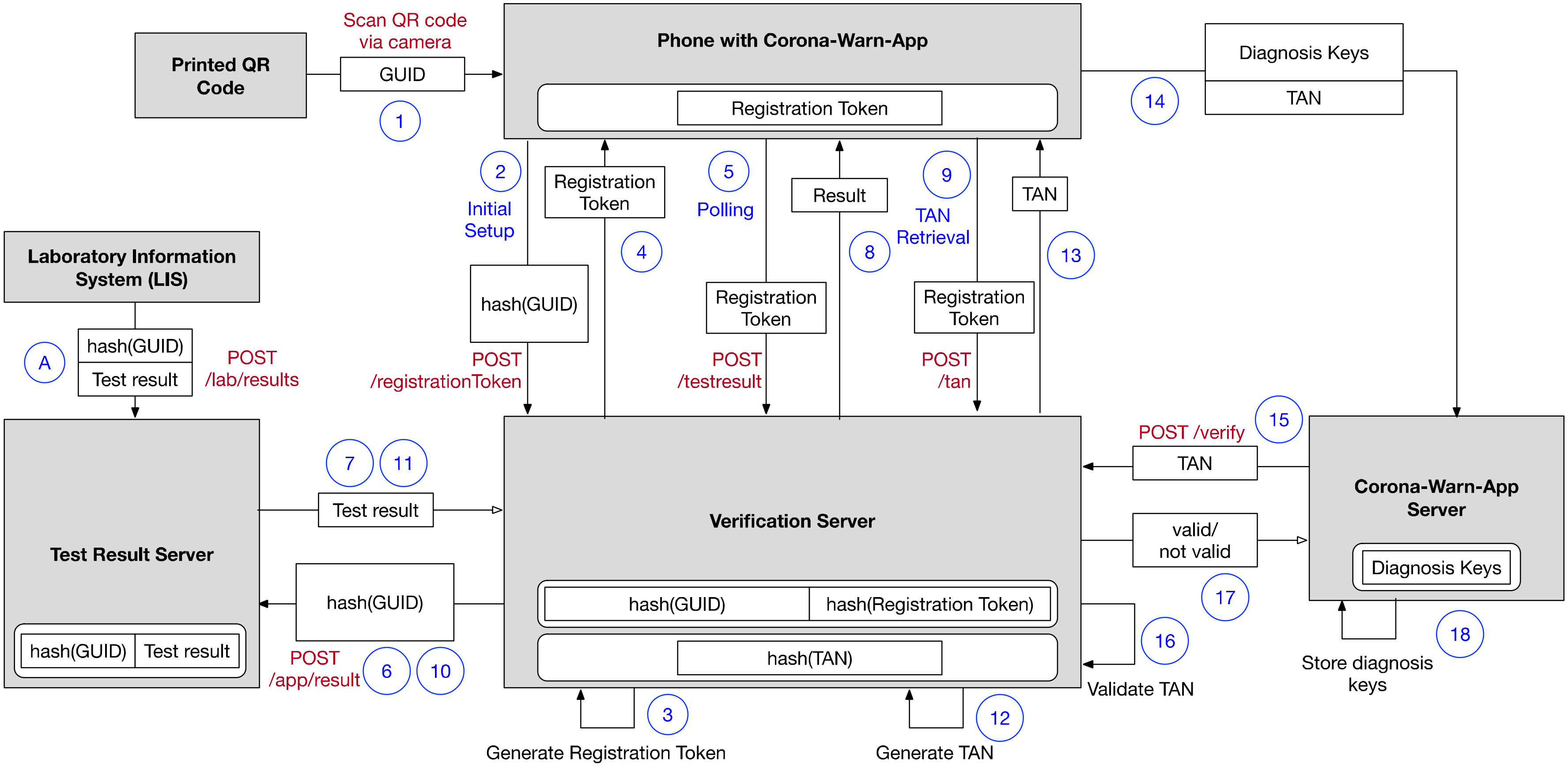
Architecture Overview


request new lab/probe ID
Test lab processing samples (Lab Client)
R
R
submit result
Laboratory Information System (LIS)
R
Open TelekomCloud (OTC)
Test results hash(GUID)
Test Result Server
R
hash(GUID) hash(Reg. Token)
hash(TAN)
Verification Server
Portal Server
R
R
Hotline
TAN verification
R
Database
Corona-Warn-App Server
retrieve TAN
R
R
poll test results
R
register with GUID
R
Transport Metadata Removal
Upload of keys + TAN
aggregated keys
R
Content Delivery Network (CDN)
Aggregated diagnosis keys
aggregated national keys
R
R
request foreign keys
R
callback
Database
European Federation Gateway Service (EFGS)
Mobile Phone
Trigger local notification
OS API/SDK for Push Messages (Notification Framework)
Camera
R
R
OS API/SDK for Exposure Notification (v2)
zxing QR Code Library
OS Crypto SDK
Protobuf library
R
read QR code from app (GUID)
R
R
R
Registration Token
Contact Journal Entries
Corona-Warn-App for tracing and test result retrieval (Apple iOS / Google Android)
Open Source
Operating System (OS) Component
Existing external system/library (consumed)
see more detailed documentation

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

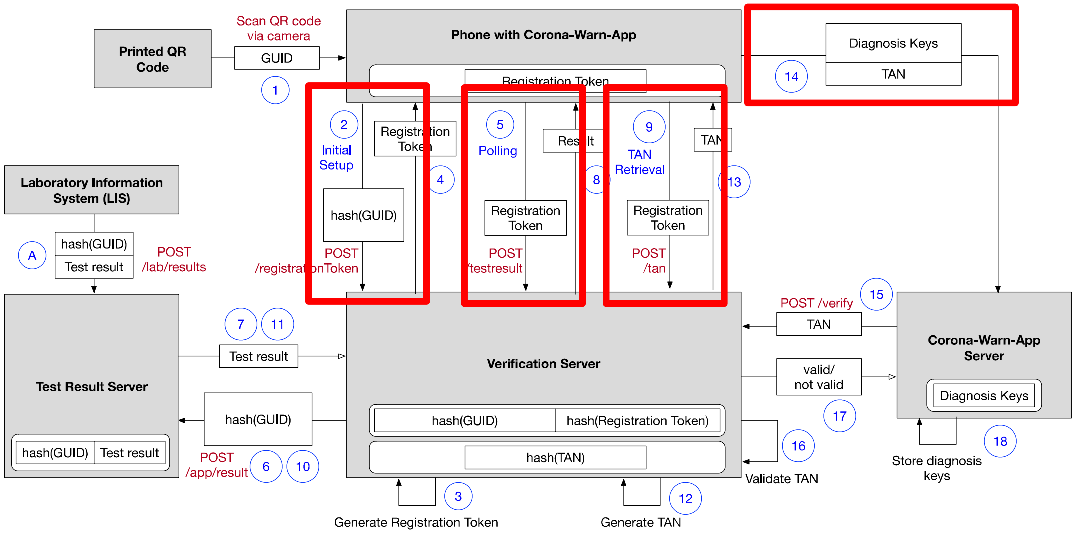
(2) The person has been tested

(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



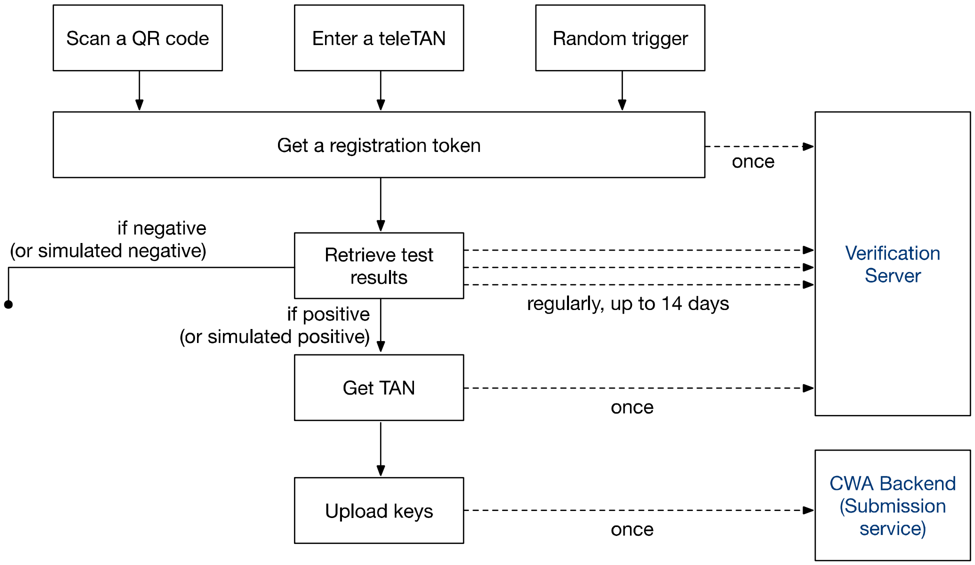
We need to establish plausible deniability

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

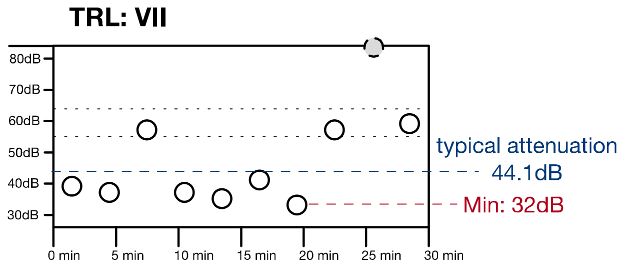
- When uploading keys, the HTTP(S) request from the mobile phone carries metadata
  - Source IP address
  - User agent (Operating System, possibly also OS version)

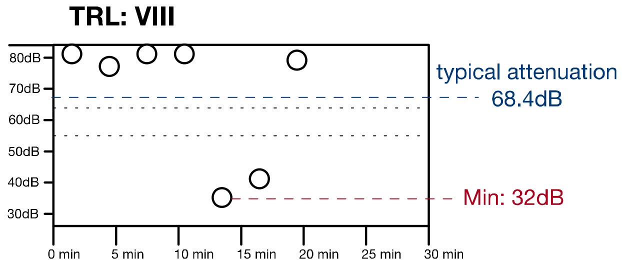
- Before the request reaches the backend server, the metadata is removed
  - only the content is forwarded to the backend service

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)

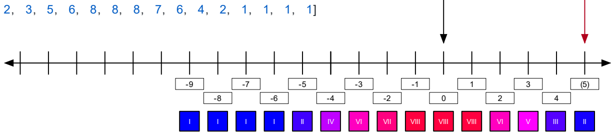
Value range (EFGS): -14 to 21

„Today is Monday.
The symptoms started last Thursday“
(5 days ago)

16.09.2020
Specifically known
onset of symptoms

21.09.2020
Submission

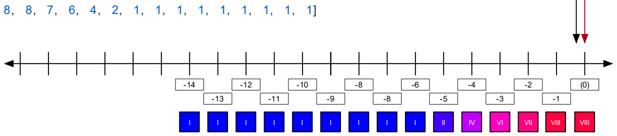
[2, 3, 5, 6, 8, 8, 8, 7, 6, 4, 2, 1, 1, 1, 1]



„Today is Monday.
The symptoms started today“
(0 days ago = smallest possible value)

21.09.2020 Submission
Specifically known
onset of symptoms

[8, 8, 7, 6, 4, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1]

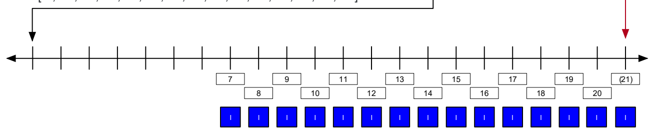


„Today is Monday.
The symptoms started last 21 days ago“
(21 days ago = largest possible value)

31.08.2020
Specifically known
onset of symptoms

21.09.2020
Submission

[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]



Transmission Risk Level

I II III IV V VI VII VIII

low high

Age of the Diagnosis Key at the point of submission (days)

Days since the onset of symptoms (at the point of submission)	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	I	I	I	I	I	I	I	I	I	II	IV	VI	VII	VIII	VIII
1	I	I	I	I	I	I	I	I	II	IV	VI	VII	VIII	VIII	VIII
2	I	I	I	I	I	I	I	II	IV	VI	VII	VIII	VIII	VIII	VI
3	I	I	I	I	I	I	II	IV	VI	VII	VIII	VIII	VIII	VI	V
4	I	I	I	I	I	II	IV	VI	VII	VIII	VIII	VIII	VI	V	III
5	I	I	I	I	II	IV	VI	VII	VIII	VIII	VIII	VI	V	III	II
6	I	I	I	II	IV	VI	VII	VIII	VIII	VIII	VI	V	III	II	II
7	I	I	II	IV	VI	VII	VIII	VIII	VIII	VI	V	III	II	II	I
8	I	II	IV	VI	VII	VIII	VIII	VIII	VI	V	III	II	II	I	I
9	II	IV	VI	VII	VIII	VIII	VIII	VI	V	III	II	II	I	I	I
10	IV	VI	VII	VIII	VIII	VIII	VI	V	III	II	II	I	I	I	I
11	VI	VII	VIII	VIII	VIII	VI	V	III	II	II	I	I	I	I	I
12	VII	VIII	VIII	VIII	VI	V	III	II	II	I	I	I	I	I	I
13	VIII	VIII	VIII	VI	V	III	II	II	I	I	I	I	I	I	I
14	VIII	VIII	VI	V	III	II	II	I	I	I	I	I	I	I	I
15	VIII	VI	V	III	II	II	I	I	I	I	I	I	I	I	I
16	VI	V	III	II	II	I	I	I	I	I	I	I	I	I	I
17	V	III	II	II	I	I	I	I	I	I	I	I	I	I	I
18	III	II	II	I	I	I	I	I	I	I	I	I	I	I	I
19	II	II	I	I	I	I	I	I	I	I	I	I	I	I	I
20	II	I	I	I	I	I	I	I	I	I	I	I	I	I	I
21	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I

Deriving the Transmission Risk Level from
Days since Onset of Symptoms (day range is known)

Value range (EFGS): 186 to 1921

Transmission Risk Level

I II III IV V VI VII VIII

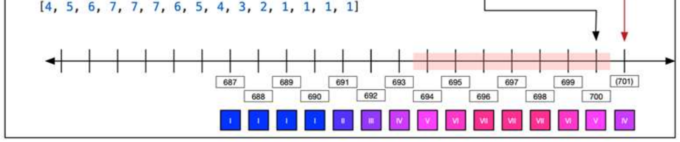
low high

„Today is Monday.
The symptoms started within the last week“
(i.e. 7 day range from 14.09.-20.09.)

20.09.2020
Last (youngest) day
of onset range

21.09.2020
Submission

[4, 5, 6, 7, 7, 7, 6, 5, 4, 3, 2, 1, 1, 1, 1]

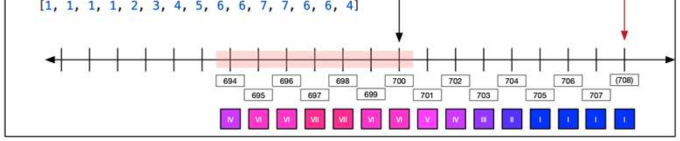


„Today is Monday.
The symptoms started 1-2 weeks ago“
(i.e. 7 day range from 07.09.-13.09.)

13.09.2020
Last (youngest) day
of onset range

21.09.2020
Submission

[1, 1, 1, 1, 2, 3, 4, 5, 6, 6, 7, 7, 6, 6, 4]

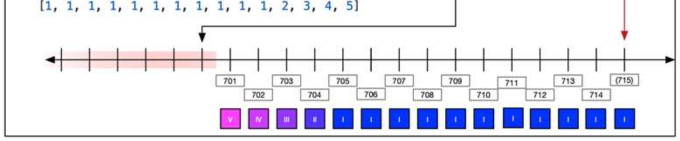


„Today is Monday.
The symptoms started >2 weeks ago“
(7 day range from 31.08.-06.09.)

06.09.2020
Last (youngest) day
of onset range

21.09.2020
Submission

[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 3, 4, 5]



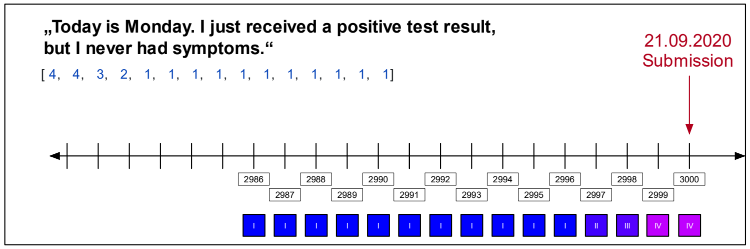
Transmission Risk Level - based on symptom status

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

Transmission Risk Level

I II III IV V VI VII VIII

low high



„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, 1, 1]

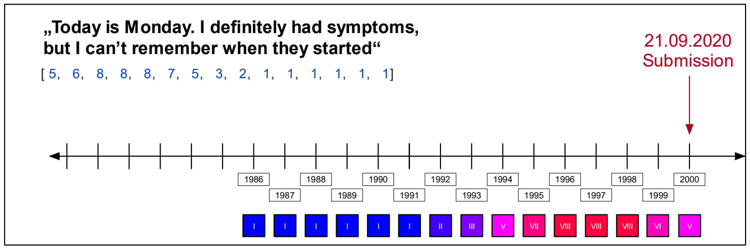
21.09.2020
Submission

Deriving the Transmission Risk Level from
Days since Onset of Symptoms (onset day **not** known)
—> technically „days since submission“
Value range (EFGS): 1986 to 2000

Transmission Risk Level

I II III IV V VI VII VIII

low high



„Today is Monday. I definitely had symptoms, but I can't remember when they started“

[5, 6, 8, 8, 8, 7, 5, 3, 2, 1, 1, 1, 1, 1, 1]

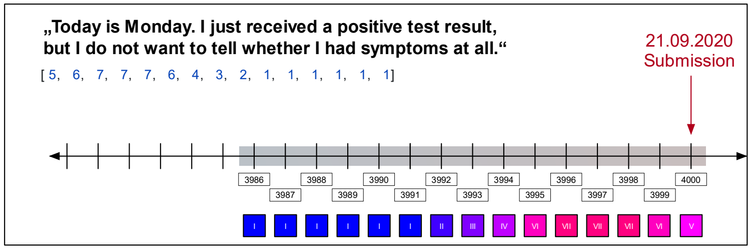
21.09.2020
Submission

Deriving the Transmission Risk Level from
Days since Onset of Symptoms (no information)
—> technically „days since submission“
Value range (EFGS): 3986 to 4000

Transmission Risk Level

I II III IV V VI VII VIII

low high

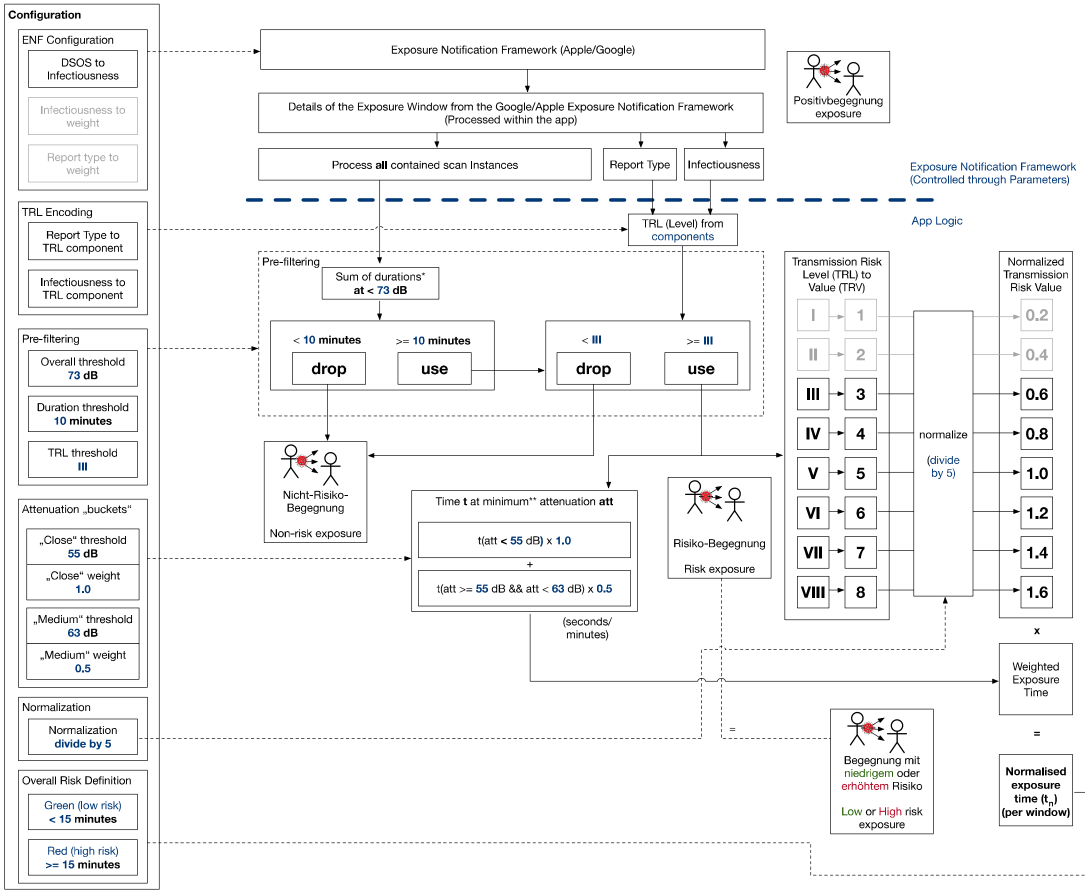


„Today is Monday. I just received a positive test result, but I do not want to tell whether I had symptoms at all.“

[5, 6, 7, 7, 7, 6, 4, 3, 2, 1, 1, 1, 1, 1, 1]

21.09.2020
Submission

Risk calculation



Configuration

ENF Configuration
DSOS to Infectiousness
Infectiousness to weight
Report type to weight

TRL Encoding
Report Type to TRL component
Infectiousness to TRL component

Pre-filtering
Overall threshold **73 dB**
Duration threshold **10 minutes**
TRL threshold **III**

Attenuation „buckets“
„Close“ threshold **55 dB**
„Close“ weight **1.0**
„Medium“ threshold **63 dB**
„Medium“ weight **0.5**

Normalization
Normalization **divide by 5**

Overall Risk Definition
Green (low risk) **< 15 minutes**
Red (high risk) **>= 15 minutes**

Exposure Notification Framework (Apple/Google)

Details of the Exposure Window from the Google/Apple Exposure Notification Framework (Processed within the app)

Process **all** contained scan Instances
Report Type
Infectiousness

Positivbegegnung exposure

Exposure Notification Framework (Controlled through Parameters)

App Logic

TRL (Level) from components

Pre-filtering
Sum of durations* **at < 73 dB**
< **10 minutes** — **drop**
>= **10 minutes** — **use**
< **III** — **drop**
>= **III** — **use**

Nicht-Risiko-Begegnung
Non-risk exposure

Time **t** at minimum** attenuation **att**
t(att **< 55** dB) x **1.0**
+
t(att >= **55** dB && att < **63** dB) x **0.5**
(seconds/ minutes)

Risiko-Begegnung
Risk exposure

Transmission Risk Level (TRL) to Value (TRV)			Normalized Transmission Risk Value
I	1	normalize (divide by 5)	0.2
II	2		0.4
III	3		0.6
IV	4		0.8
V	5		1.0
VI	6		1.2
VII	7		1.4
VIII	8		1.6

x

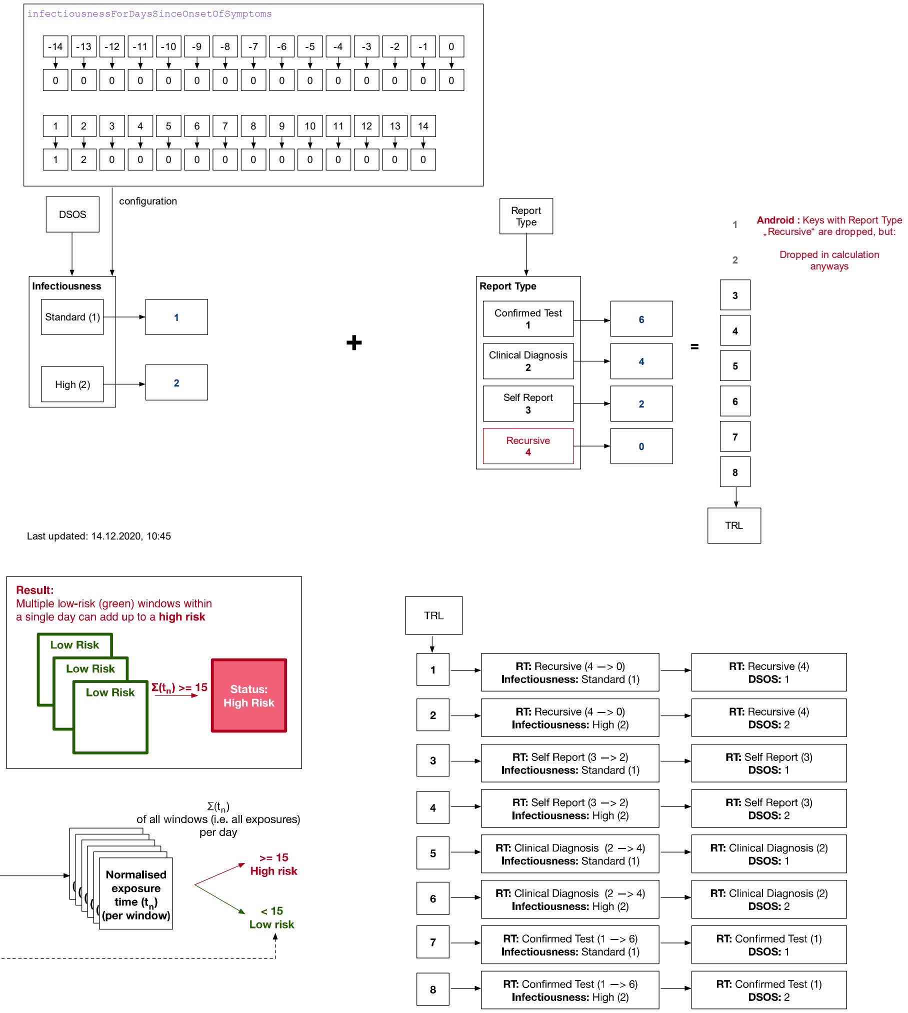
Weighted Exposure Time

=

Normalised exposure time (t_n) (per window)

=

Begegnung mit niedrigem oder erhöhtem Risiko
Low or High risk exposure



`infectiousnessForDaysSinceOnsetOfSymptoms`

-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	0	0	0	0	0	0	0	0	0	0	0	0

DSOS
configuration

Infectiousness	
Standard (1)	1
High (2)	2

Last updated: 14.12.2020, 10:45

+

Report Type

Report Type	
Confirmed Test 1	6
Clinical Diagnosis 2	4
Self Report 3	2
Recursive 4	0

=

1 **Android :** Keys with Report Type „Recursive“ are dropped, but:
2 Dropped in calculation anyways
3
4
5
6
7
8

TRL

Result:
Multiple low-risk (green) windows within a single day can add up to a **high risk**

Low Risk
Low Risk
Low Risk
$\Sigma(t_n)$ >= 15
Status: High Risk

$\Sigma(t_n)$
of all windows (i.e. all exposures) per day

Normalised exposure time (t_n) (per window)

>= 15 High risk
< 15 Low risk

TRL

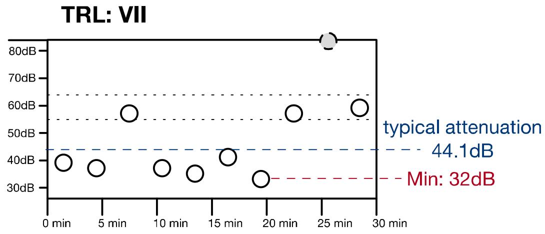
1	**RT:** Recursive (4 —> 0) **Infectiousness:** Standard (1)	**RT:** Recursive (4) **DSOS:** 1
2	**RT:** Recursive (4 —> 0) **Infectiousness:** High (2)	**RT:** Recursive (4) **DSOS:** 2
3	**RT:** Self Report (3 —> 2) **Infectiousness:** Standard (1)	**RT:** Self Report (3) **DSOS:** 1
4	**RT:** Self Report (3 —> 2) **Infectiousness:** High (2)	**RT:** Self Report (3) **DSOS:** 2
5	**RT:** Clinical Diagnosis (2 —> 4) **Infectiousness:** Standard (1)	**RT:** Clinical Diagnosis (2) **DSOS:** 1
6	**RT:** Clinical Diagnosis (2 —> 4) **Infectiousness:** High (2)	**RT:** Clinical Diagnosis (2) **DSOS:** 2
7	**RT:** Confirmed Test (1 —> 6) **Infectiousness:** Standard (1)	**RT:** Confirmed Test (1) **DSOS:** 1
8	**RT:** Confirmed Test (1 —> 6) **Infectiousness:** High (2)	**RT:** Confirmed Test (1) **DSOS:** 2

* ∀(scan instance): att < 73 dB (Σ(secondsSinceLastScan))
** changes possible

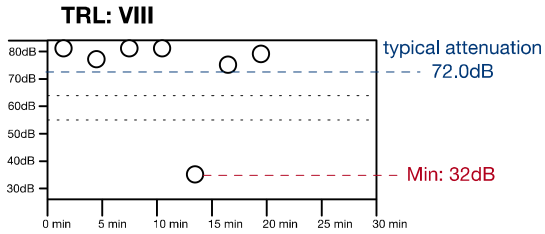
Last updated: 16.12.2020, 14:40

Last updated: 14.12.2020, 10:00

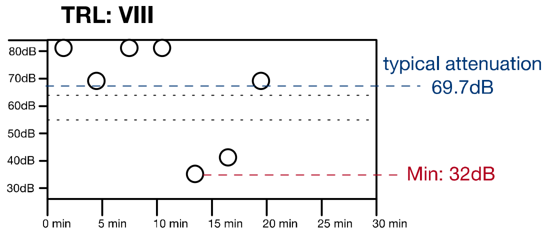
High or low risk for those windows? Red or Green?



- 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