Mobile Applications for Privacy-Preserving Digital Contact Tracing

Christos Laoudias, Steffen Meyer, Philippos Isaia, Thomas Windisch, Justus Benzler, Maximilian Lenkeit

KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia, Cyprus
Precise Positioning and Analytics Department, Fraunhofer Institute of Integrated Circuits, Nuremberg, Germany
Robert Koch Institute, Berlin, Germany
SAP SE, Technology & Innovation, Walldorf, Germany

The Advanced Seminar Team

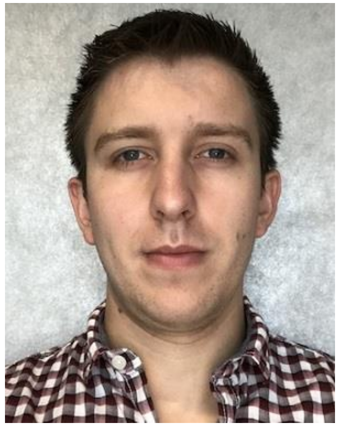
Christos Laoudias

Steffen Meyer

Philippos Isaia

Thomas Windisch

Justus Benzler



Maximilian Lenkeit

The CovTracer-EN project has received funding from the European Union's Emergency Support Instrument programme under grant agreement No. CYPRUS-LC-015948.

Disclaimer

Feel free to use any of the following slides/content for educational purposes, however kindly acknowledge the source

We would also like to know how you have used these slides, so please send us an email with comments or suggestions

Keep notes of your questions as there will be **5 minutes** for Q&A at the end of each part

Feel free to post questions in the chat box and we will try to answer them in real-time

The slides are available on Zenodo

The recording will be published on the MDM Youtube channel[1]

[1]MDM YouTube channel https://www.youtube.com/channel/UCGm81lAnc-VhAHbbzozXelA

Outline

Part 1 – Introduction to Mobile Contact Tracing Apps (MCTA)

- Introduction to Digital Contact Tracing (DCT)
- DCT technologies and systems

Part 2 – Deploying country-wide MCTA: From theory to practice

- Google/Apple Exposure Notification (GAEN) framework
- Real-life implementation: The German Corona-Warn-App system

Part 3 – Performance evaluation and what is next

- Uptake and effectiveness of MCTA
- Cybersecurity and data privacy aspects
- Recent trends and future directions

Outline

Part 1 – Introduction to Mobile Contact Tracing Apps (MCTA)

- Introduction to Digital Contact Tracing (DCT)
- DCT technologies and systems

Part 2 – Deploying country-wide MCTA: From theory to practice

- Google/Apple Exposure Notification (GAEN) framework
- Real-life implementation: The German Corona-Warn-App system

Part 3 – Performance evaluation and what is next

- Uptake and effectiveness of MCTA
- Cybersecurity and data privacy aspects
- Recent trends and future directions

Introduction to Digital Contact Tracing
Digital solutions for pandemics management

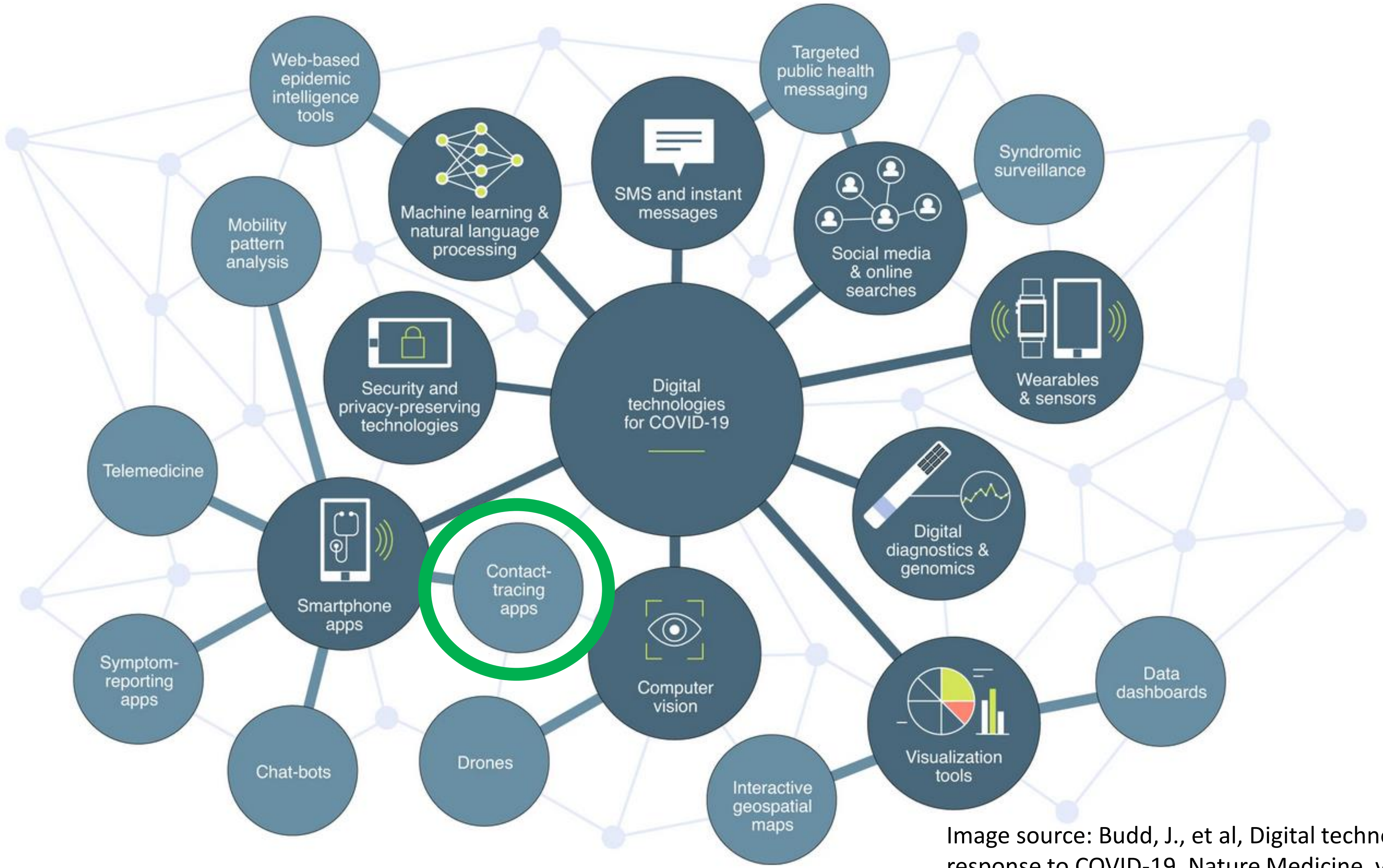


Image source: Budd, J., et al, Digital technologies in the public-health response to COVID-19, Nature Medicine, vol. 26, pp. 1183–1192, 2020.

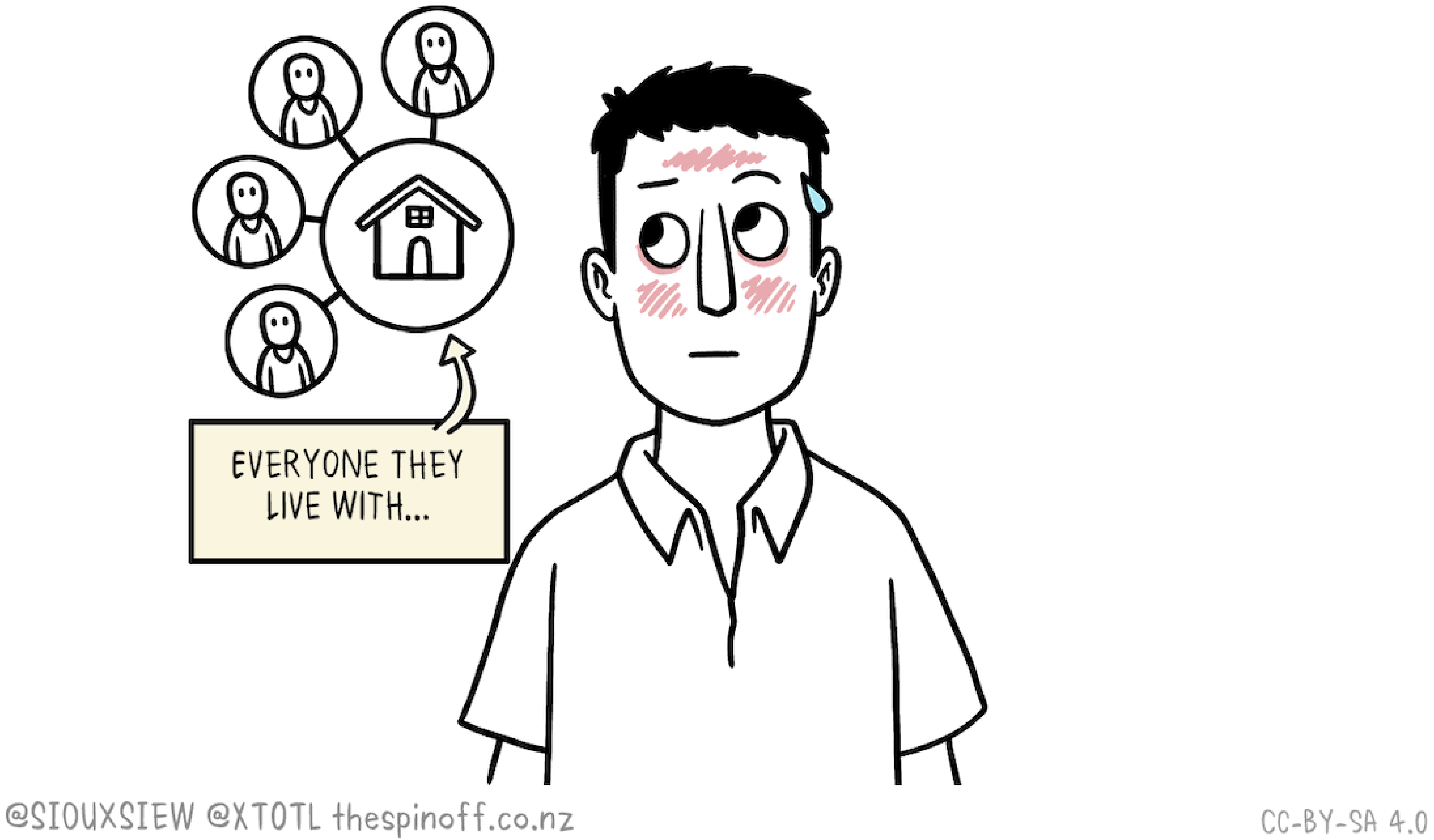
Introduction to Digital Contact Tracing
Conventional contact tracing – How does it work?

Introduction to Digital Contact Tracing

Conventional contact tracing – How does it work?

Introduction to Digital Contact Tracing

Conventional contact tracing – How does it work?



Introduction to Digital Contact Tracing

Conventional contact tracing – How does it work?

Introduction to Digital Contact Tracing

Conventional contact tracing – How does it work?

Introduction to Digital Contact Tracing
Conventional contact tracing – How does it work?

Introduction to Digital Contact Tracing
Conventional contact tracing – How does it work?

Introduction to Digital Contact Tracing

Conventional contact tracing – Limitation 1: Resource-demanding process

Army of contact tracers

- 13K – 265K tracers estimated for USA[1]
  - 100K full-time tracers for 1 year cost approx. $3.6B
- NHS Test and Trace service (late May 2020)
  - 25K contact tracing staff
  - Capacity to trace 10K contacts per day
- Germany planned for ~21K tracers before the 2nd lockdown[2]

[1]C. Watson, A national plan to enable comprehensive COVID-19 case finding and contact tracing in the US, Johns Hopkins Center for Health Security, 2020.
[2]D. Lewis, Why many countries failed at COVID contact-tracing — but some got it right, Nature News Feature, Dec. 2020.
Image source: Bryan Anselm/NYT/Redux/eyevine

Introduction to Digital Contact Tracing

Conventional contact tracing – Limitation 2: Scalability

Inefficient when applied **at large** and for a **high volume** of positive cases

- Every minute counts in breaking the infection chains
- The interview with every positively-tested citizen introduces delays in identifying close and risky contacts

Image source: Health-care workers conduct contact-tracing amid the COVID-19 pandemic in Soyapango, El Salvador, in July. Credit: Jose Cabezas/Reuters

Introduction to Digital Contact Tracing

Conventional contact tracing – Limitation 3: Hidden infections

Contacts with colleagues and acquaintance can be missed

Risky contacts with unknown individuals

Close contacts with family and fiends are usually easy to recall

Introduction to Digital Contact Tracing
How does DCT help?

"Analog" solutions
- Logbook of contacts
- Signing up when entering and exiting indoor/outdoor spaces

Digital solutions
- Telco Big Data
- Mobile Contact Tracing Apps (MCTA)
  - GPS location tracking
  - Bluetooth proximity tracing

Introduction to Digital Contact Tracing
How does DCT help?

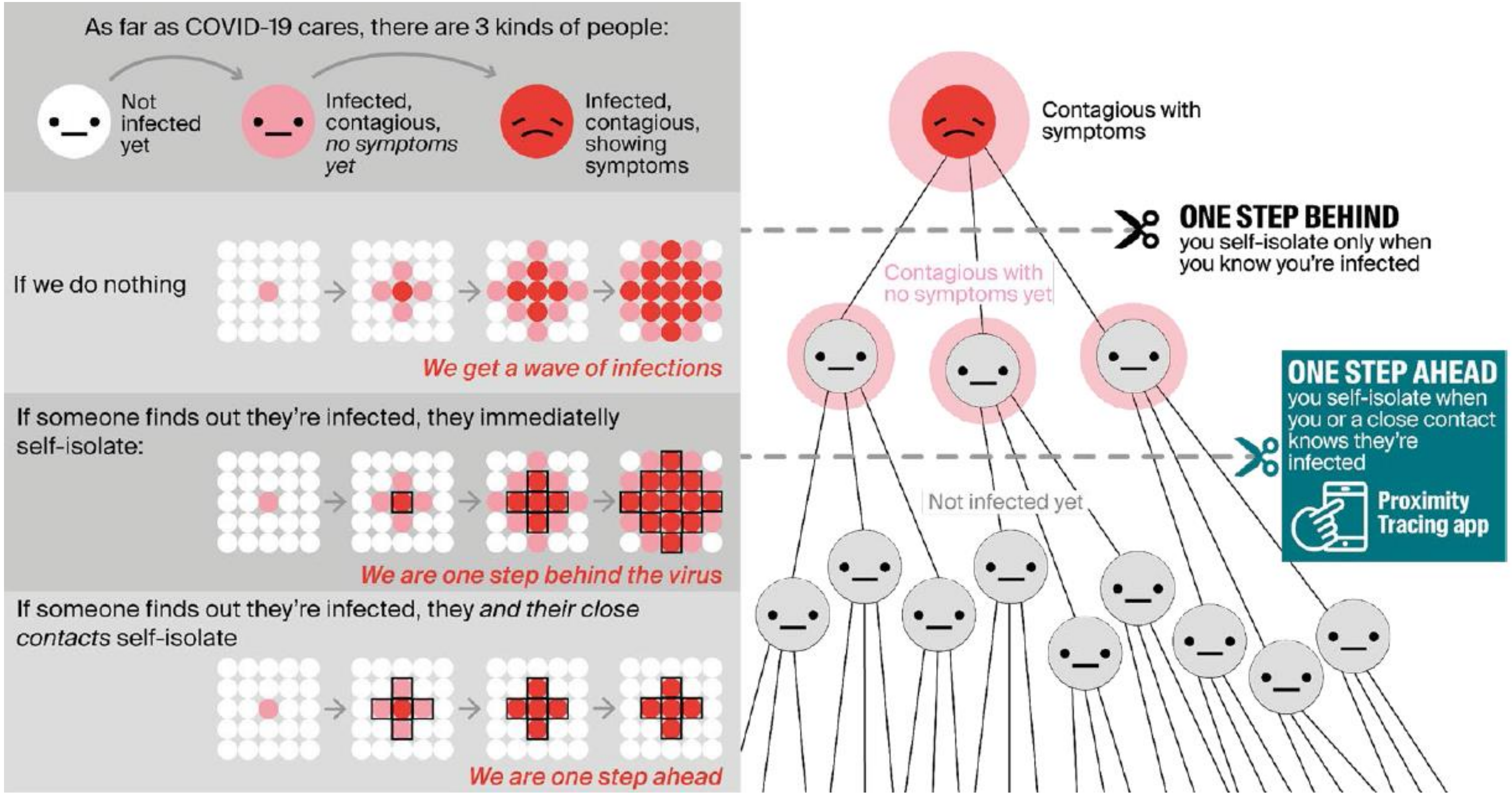
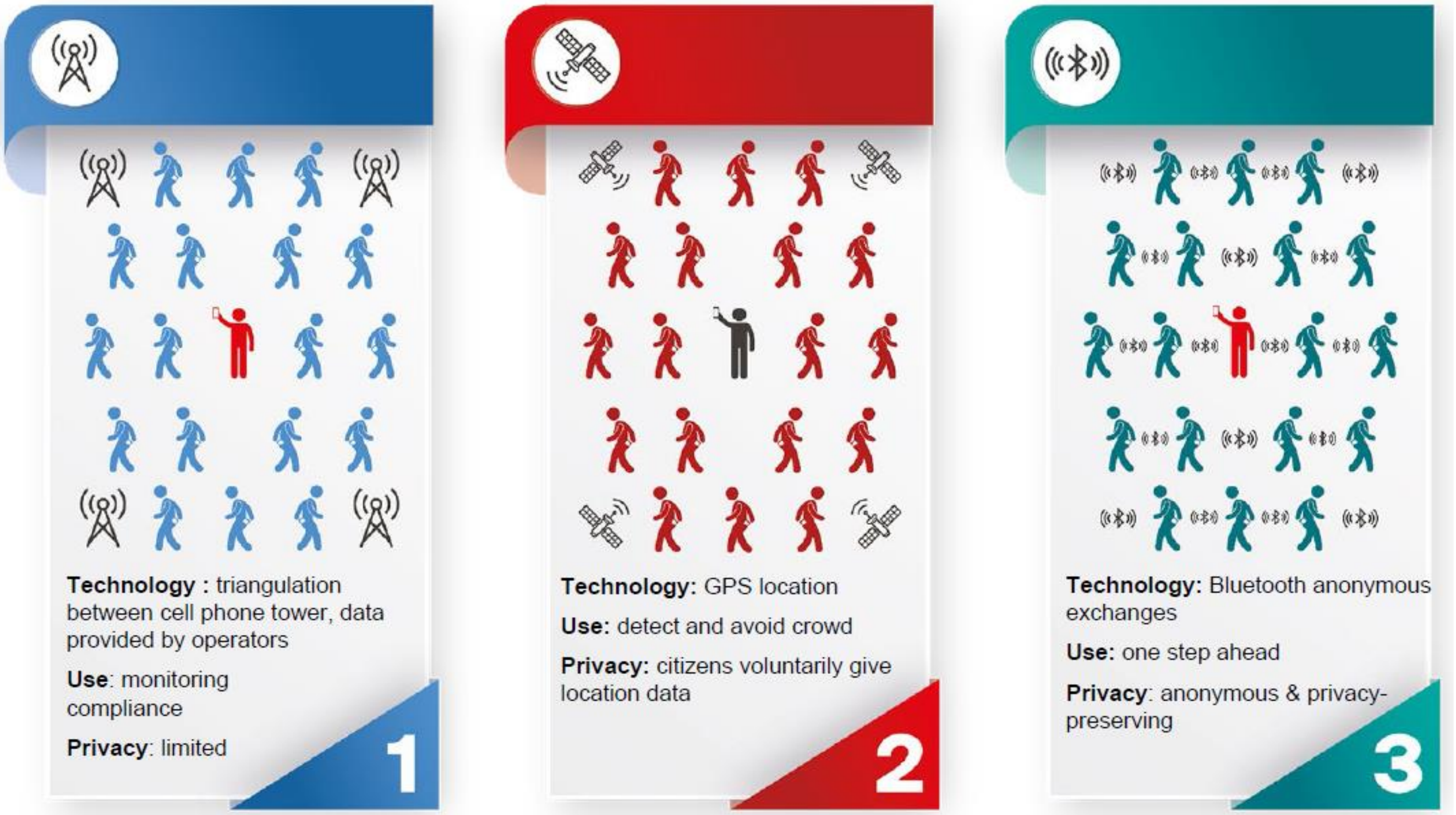


Image source: https://github.com/DP-3T/documents/

Evolution of Digital Contact Tracing



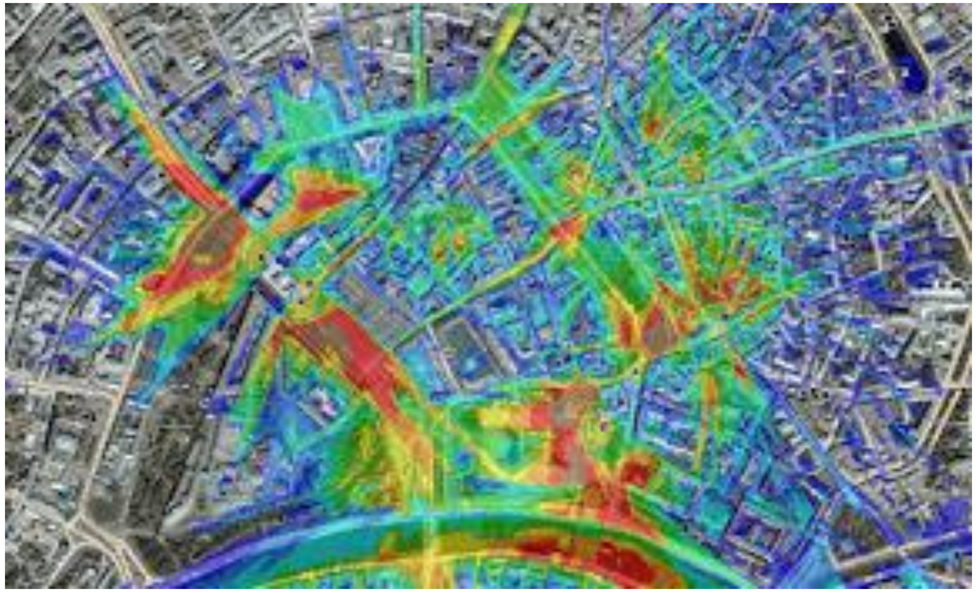
Centralized approach

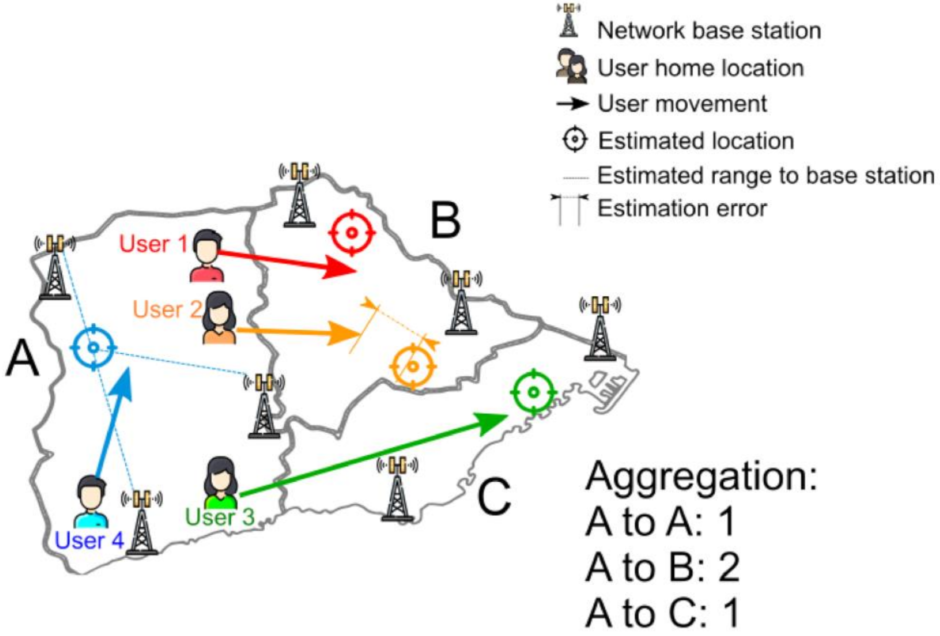
Decentralized approach

Hybrid approach

Source: https://github.com/DP-3T/documents/

Evolution of DCT
1G: Telco Big Data





☺ Health authorities can monitor the evolution of the pandemic[1]
- identify/predict infection hotspots
- monitor the mobility among geographical areas
- assess the effectiveness and degree of (non-)compliance to restrictions

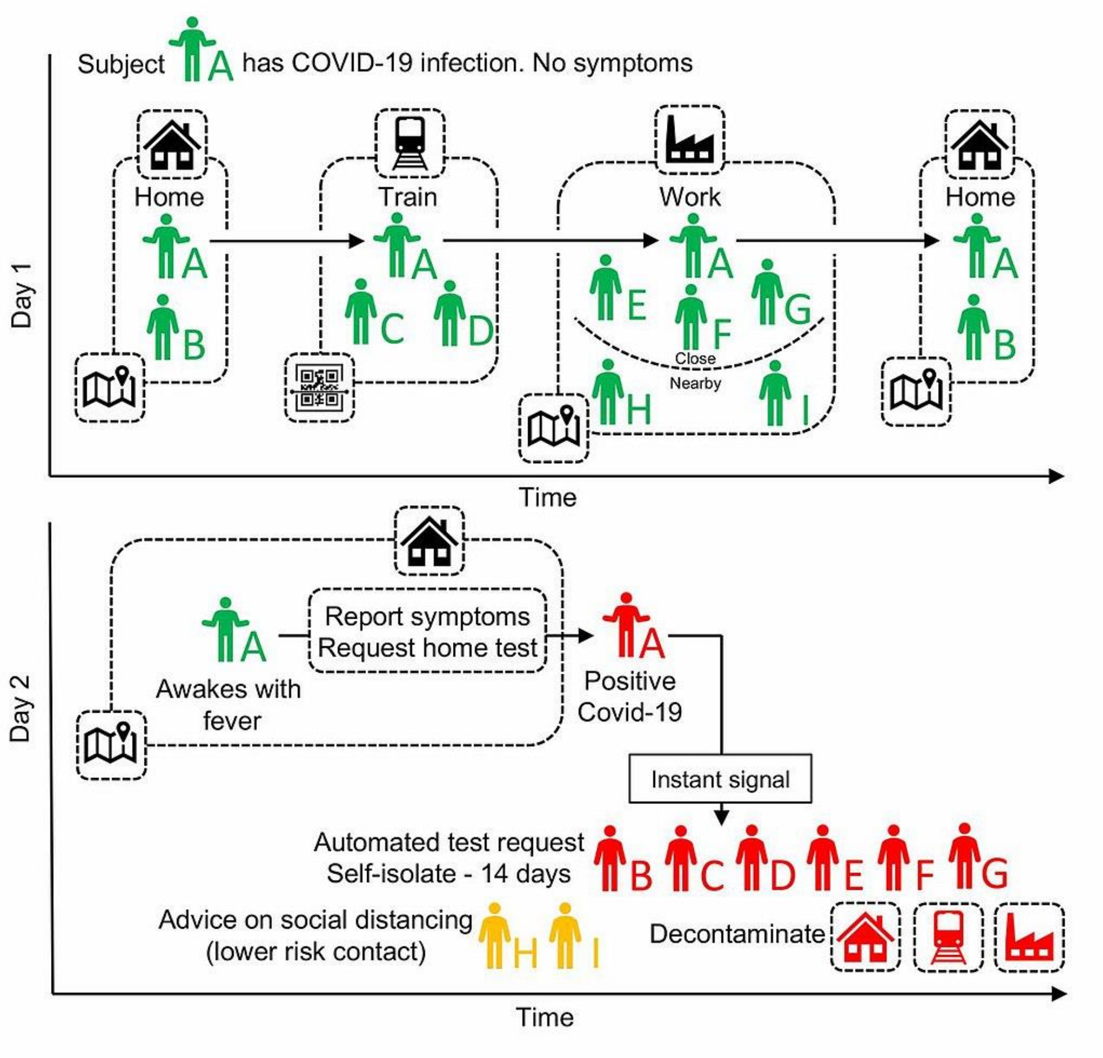
☹ Limited privacy

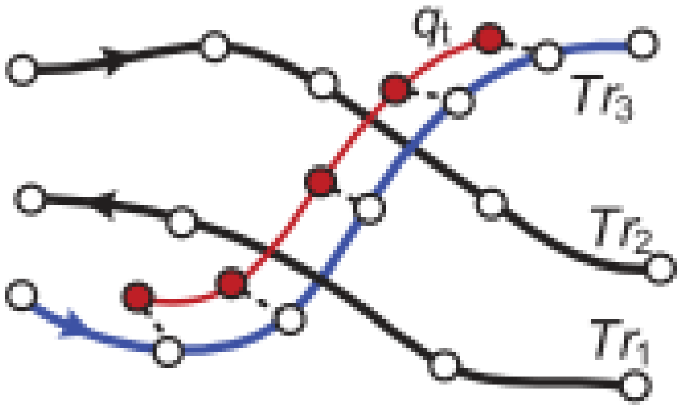
South Korea combined Telco Big Data with credit cards transactions
- Reduced the contact tracing time for a confirmed case from **>24h** to **<10min**

[1]Emil J. Khatib et al., Mass Tracking in Cellular Networks for the COVID-19 Pandemic Monitoring, Sensors 21, no. 10: 3424, 2021.
[2]Lee, G. and Kim, J., Delivering a rapid digital response to the COVID-19 pandemic. *Communications of the ACM*, *65*(1), pp.68-75, 2021.

Evolution of DCT

2G: Mobile Contact Tracing Apps – GPS location tracking





Aarogya Setu

मैं सुरक्षित | हम सुरक्षित | भारत सुरक्षित

HaMagen 2.0

sends a notification of exposure to keep you and your family safe

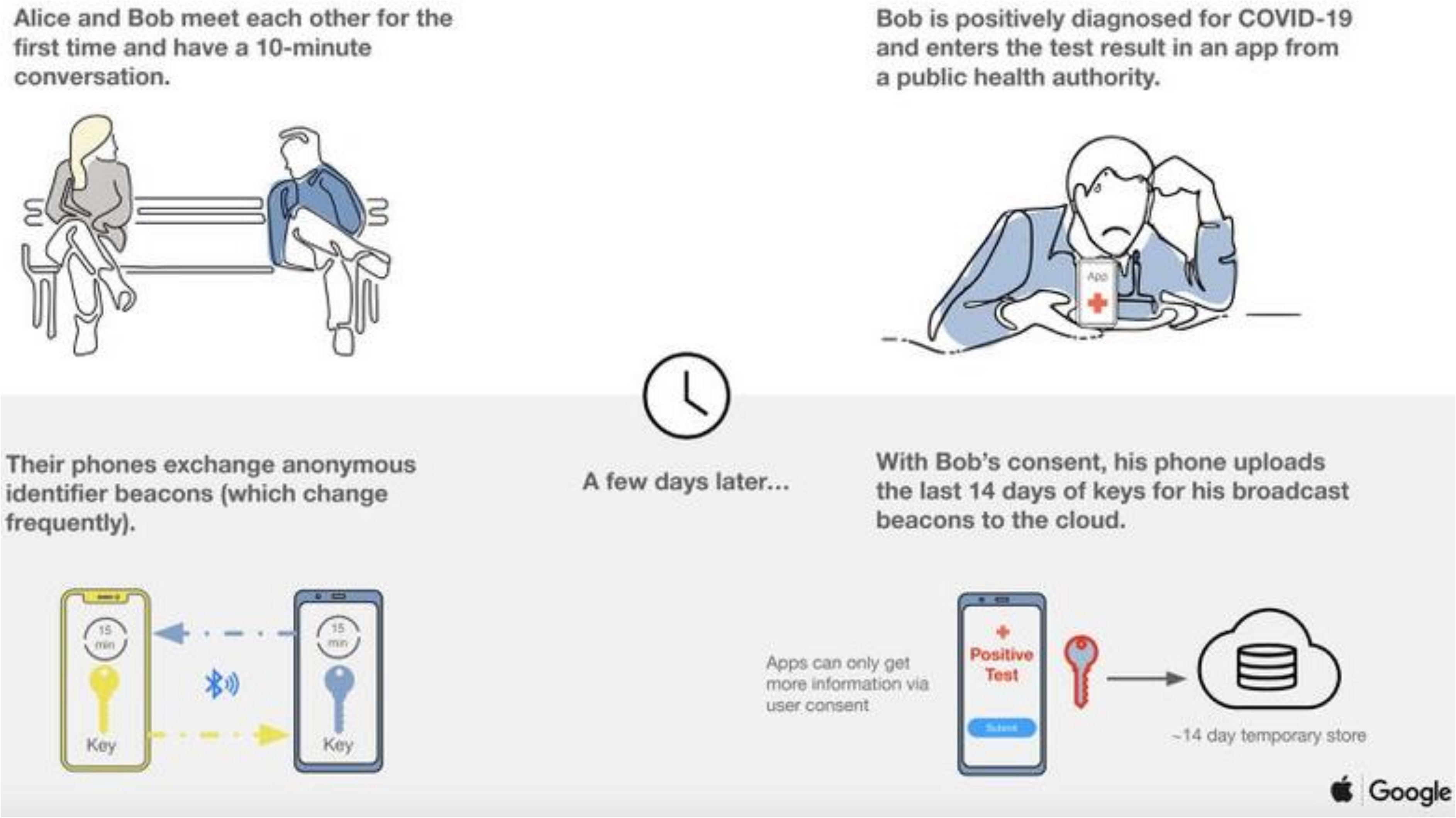
Together we can defeat Covid-19!

- ☺ Location data stored locally on the user's device unless released for tracing purposes in the case of an infection
- ☹ Still reveal to the health authorities more information (e.g., visited locations) that is necessary for contact tracing
- ☹ Limited availability indoors

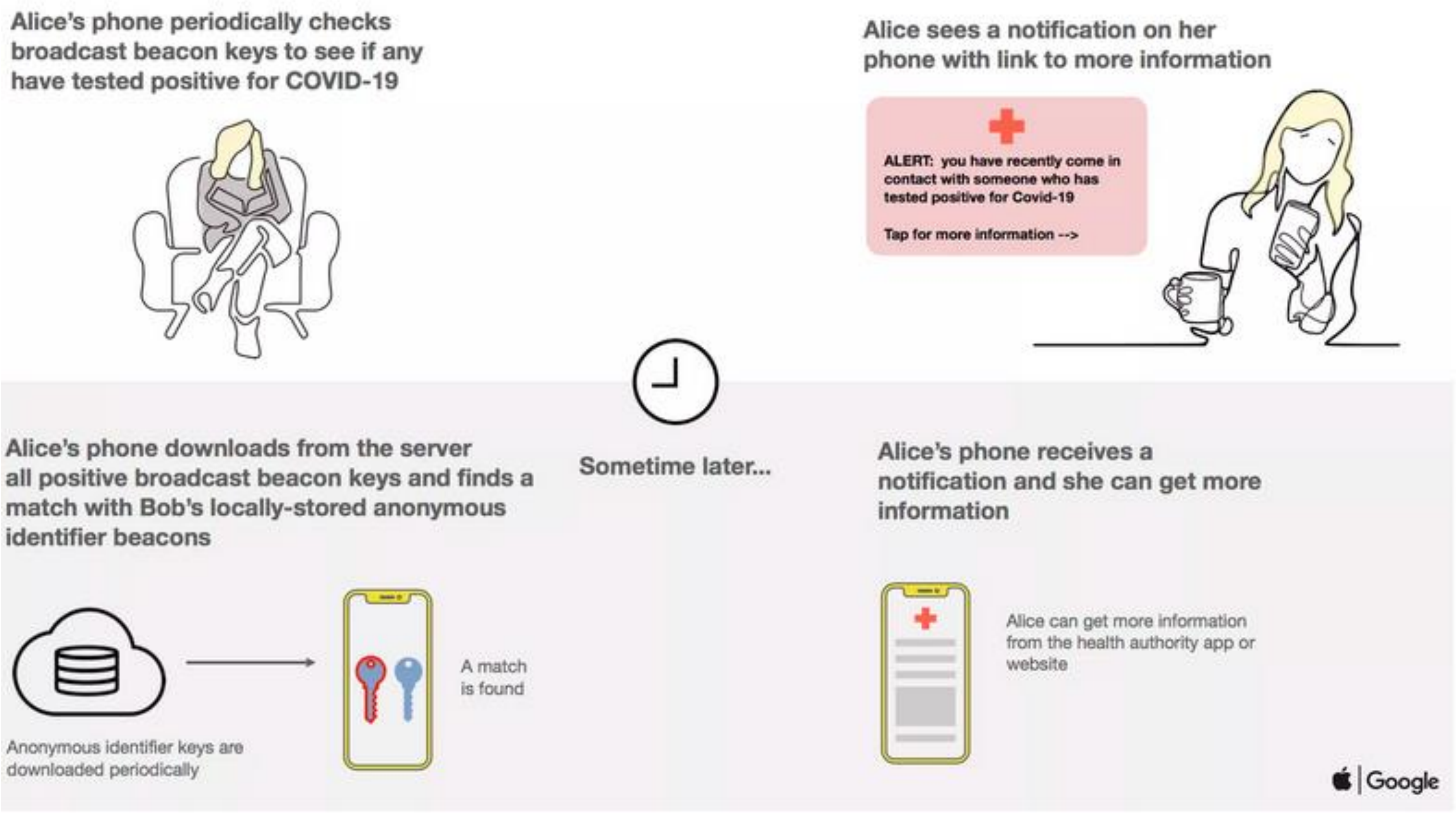
Image source: L. Ferretti et al., Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science, 2020.

Evolution of DCT

3G: Mobile Contact Tracing Apps – Bluetooth proximity tracing



Evolution of DCT
3G: Mobile Contact Tracing Apps – Bluetooth proximity tracing



Evolution of DCT
3G: Mobile Contact Tracing Apps – Centralized vs. Decentralized proximity tracing

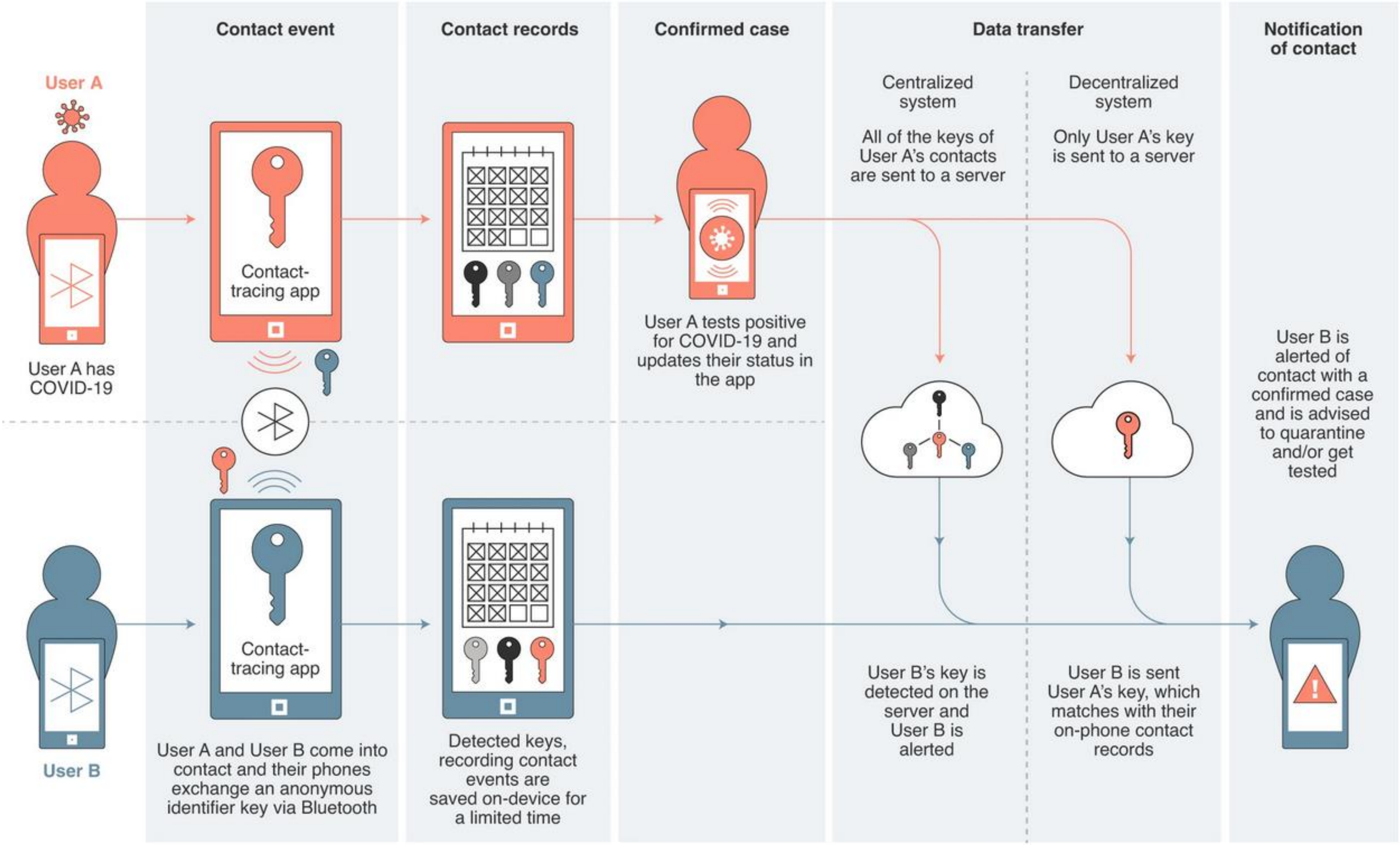


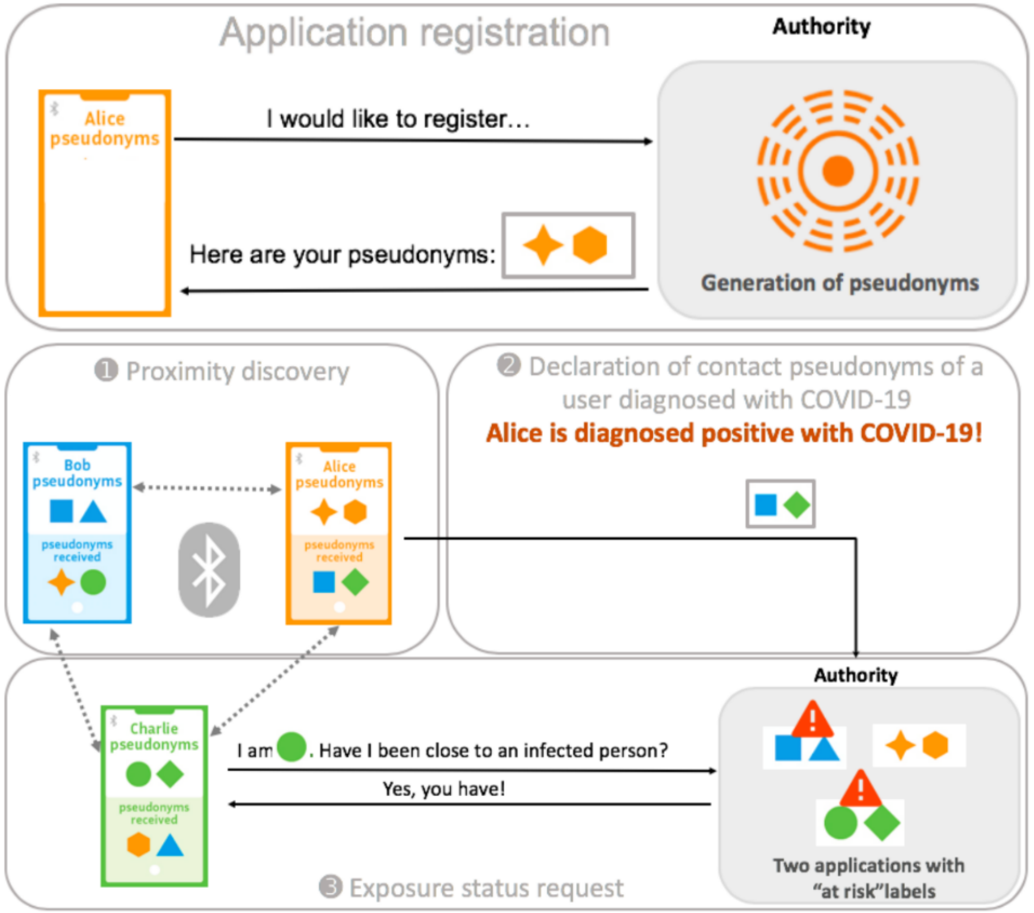
Image source: Budd, J., et al, Digital technologies in the public-health response to COVID-19, Nature Medicine, vol. 26, pp. 1183–1192, 2020.

Evolution of DCT technologies and systems
Bluetooth-based protocols: Centralized – ROBERT

ROBust and privacy-presERving proximity Tracing

- Protocol for digital contact tracing via Bluetooth
- Phone gets pseudonyms by registering at the health authority
- Using Bluetooth, the phones change pseudonyms
- If a person is tested positive, the health authority can be informed
- All other phones which are using ROBERT query the authority database with the recorded/seen pseudonyms

If a phone was in close distance to an infected person (pseudonyms has been recorded), the phone and the authority are informed.



Source: https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-summary-EN.pdf

Evolution of DCT technologies and systems
Bluetooth-based protocols: Decentralized – DP-3T

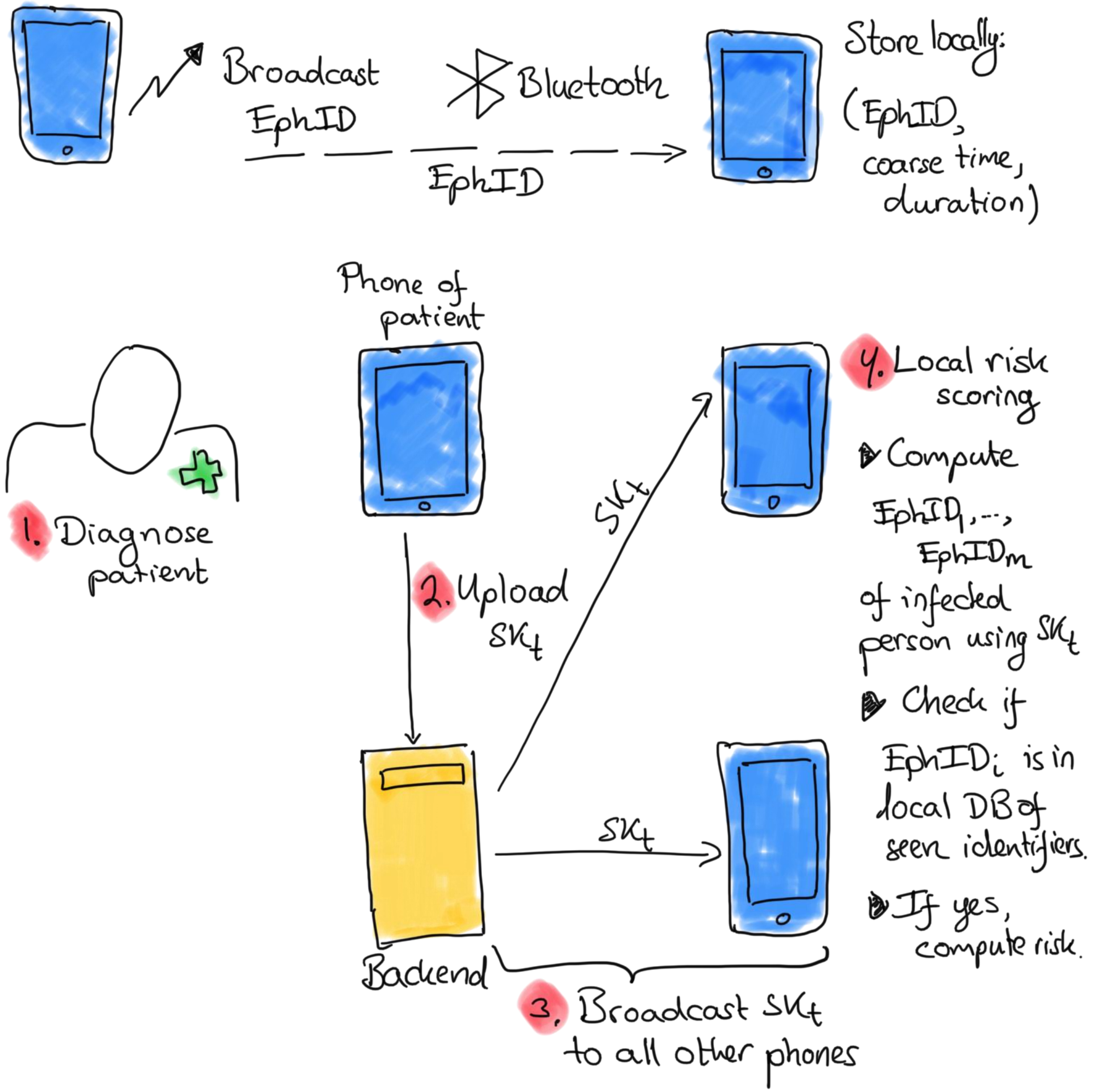
Decentralized Privacy-Preserving Proximity Tracing

EphID: Ephemeral Bluetooth identifier

- Series of daily EphIDs created by using a secret day seed key SK_t, a pseudorandom function (e.g., HMAC-SHA256) and a pseudorandom generator (e.g. AES in counter mode)
- Each EphID is broadcast for L minutes (i.e., epoch system parameter)

Time: Day on which this beacon was received (e.g., “April 2”)

Exposure measurement: e.g., signal attenuation



Outline

Part 1 – Introduction to Mobile Contact Tracing Apps (MCTA)

- Introduction to Digital Contact Tracing (DCT)
- DCT technologies and systems

Part 2 – Deploying country-wide MCTA: From theory to practice

- Google/Apple Exposure Notification (GAEN) framework
- Real-life implementation: The German Corona-Warn-App system

Part 3 – Performance evaluation and what is next

- Uptake and effectiveness of MCTA
- Cybersecurity and data privacy aspects
- Recent trends and future directions

Google/Apple Exposure Notification (GAEN) framework

Cross-device interoperability: Works seamlessly between Android and iPhones

Secure Bluetooth scanning and message exchange with nearby devices

- AES128-based encryption

Similar to DP-3T and TCN protocols

- 16-byte random day Temporary Exposure Key (TEK), Rolling Proximity Identifier (RPI), …

Implemented at the OS level through an API

- More efficient operation as a background process

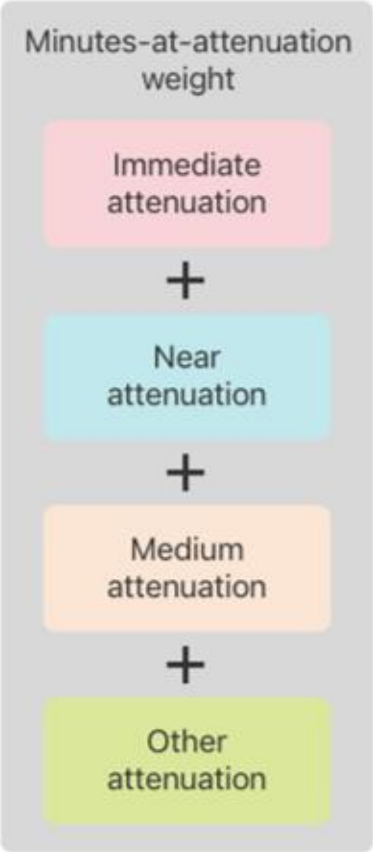
Decentralized exposure risk score calculation

Can reliably detect contacts of duration at least ~5 minutes[1]

[1]Philipp H. Kindt, et al., How reliable is smartphone-based electronic contact tracing for COVID-19? ACM Communications, vol. 65, no. 1, January 2022, 56–67.

How is the risk score calculated?

Risk score function: Combination of 3 weights



How far was I from the positive user (distance estimated through Bluetooth attenuation)?

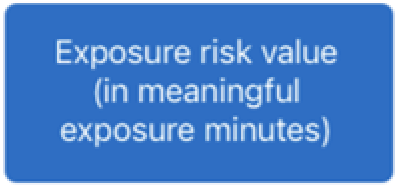
×

How many days before the positive user's symptoms onset date did I encounter him/her?

×

How did that user report his/her positive result?

=



If the exposure exceeds a predefined threshold in minutes then a notification is triggered

Configuring Bluetooth attenuations

		Immediate	Near	Medium	Other
Narrower Net 1.0	*Threshold*	<55 dB	<63 dB	<70 dB	--
	Weight	150%	100%	40%	0%
Wider Net 1.0	*Threshold*	<55 dB	<70 dB	<80 dB	--
	Weight	200%	100%	25%	0%

Immediate	Near	Medium	Other
≤55 dB	≤67 dB	≤75 dB	--
175%	100%	33%	0%

The Narrow Net v2.0 configuration addresses the updated transmission curve of the Delta variant

Narrower Net prioritizes specificity → **Fewer notifications are triggered**

- Captures some fraction of close contacts and limits the number of further-distance exposures captured

Wider Net prioritizes sensitivity → **More notifications are triggered**

- Captures most close-contact exposures and a non-negligible amount of further-distance exposures

Source: https://github.com/lfph/gaen-risk-scoring/blob/main/risk-scoring.md

Configuring infectiousness

	Narrower net	Wider net
Symptom Onset Map	*None*: days -14 to -4; days +5 to +14 *Standard*: day -3; day +4 *High*: days -2 to +3	*None*: days -14 to -6; days +10 to +14 *Standard*: -5 to -4 days; days +5 to +9 *High*: days -3 to +4
Standard weight	30%	60%
High weight	100%	200%

Revisited to address the Delta variant

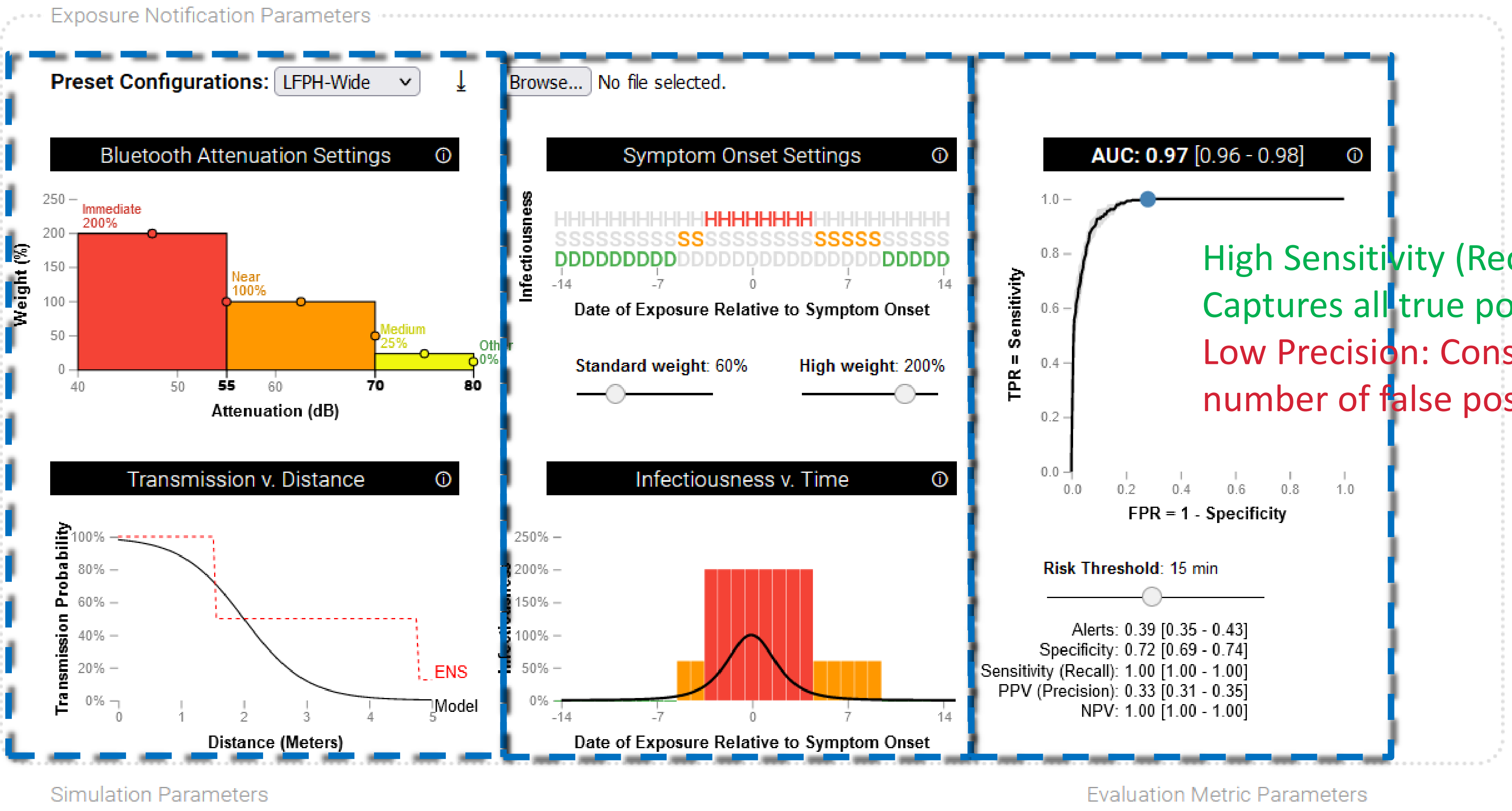
Narrower Net prioritizes **specificity**

- **Fewer notifications** restricting to exposures during the period of peak infectiousness

Wider Net prioritizes **sensitivity**

- **More notifications** capturing exposures over a longer period of potential infectiousness

COVID-19 Risk Score Tuner – Wider net



High Sensitivity (Recall): Captures all true positives

Low Precision: Considerable number of false positives

Source: Murphy, K., Kumar, A. and Serghiou, S., 2021. Risk score learning for COVID-19 contact tracing apps. arXiv preprint arXiv:2104.08415.
https://risk-score-tuner.appspot.com/

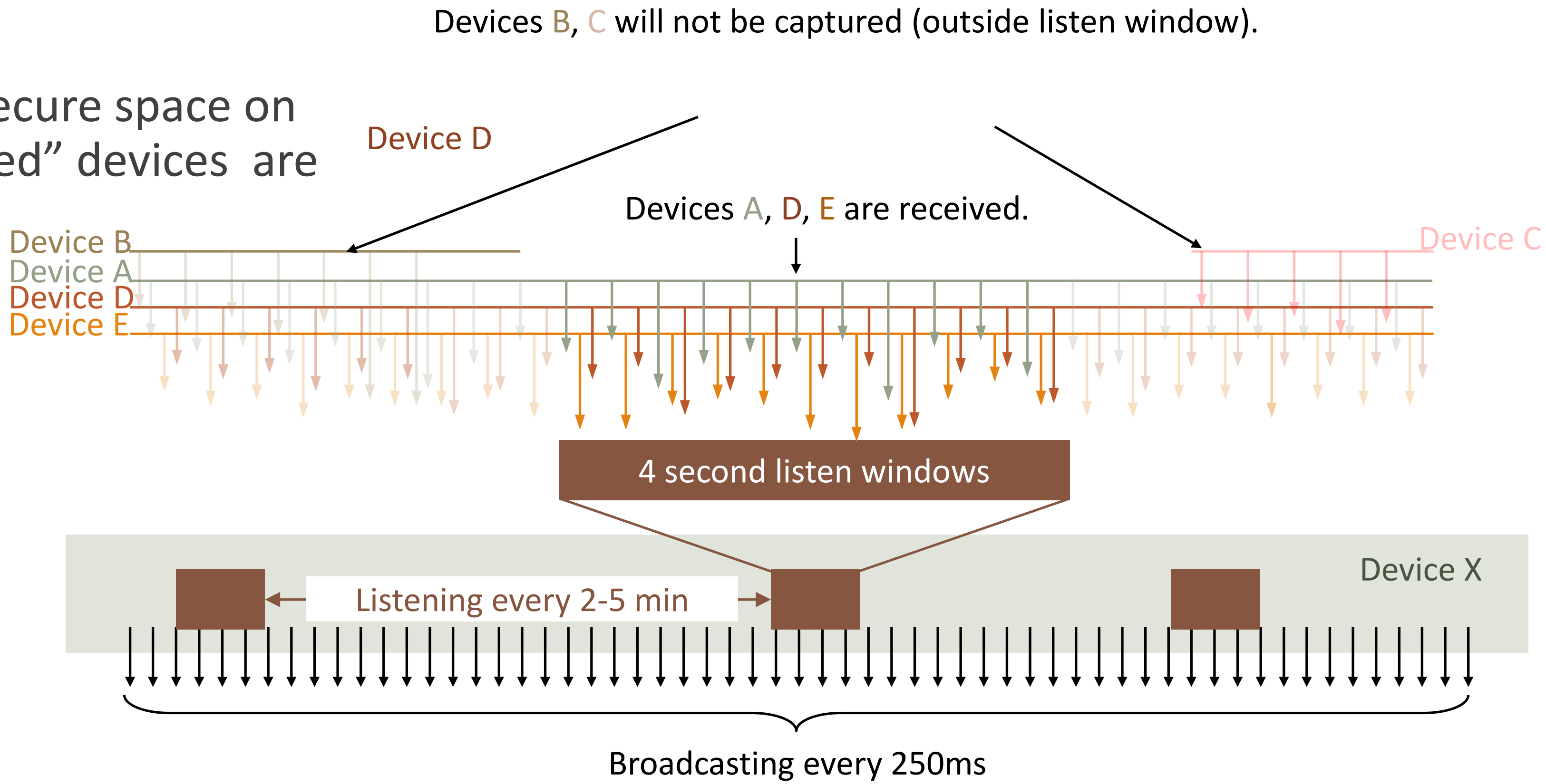
GAEN V2: Advanced Features

Devices broadcast every 250 ms and listen for 4 seconds every 2-5 minutes.

Received beacons are stored in a secure space on the device, only beacons of "infected" devices are further processed.

For each listening window a "Scan Instance" is created:

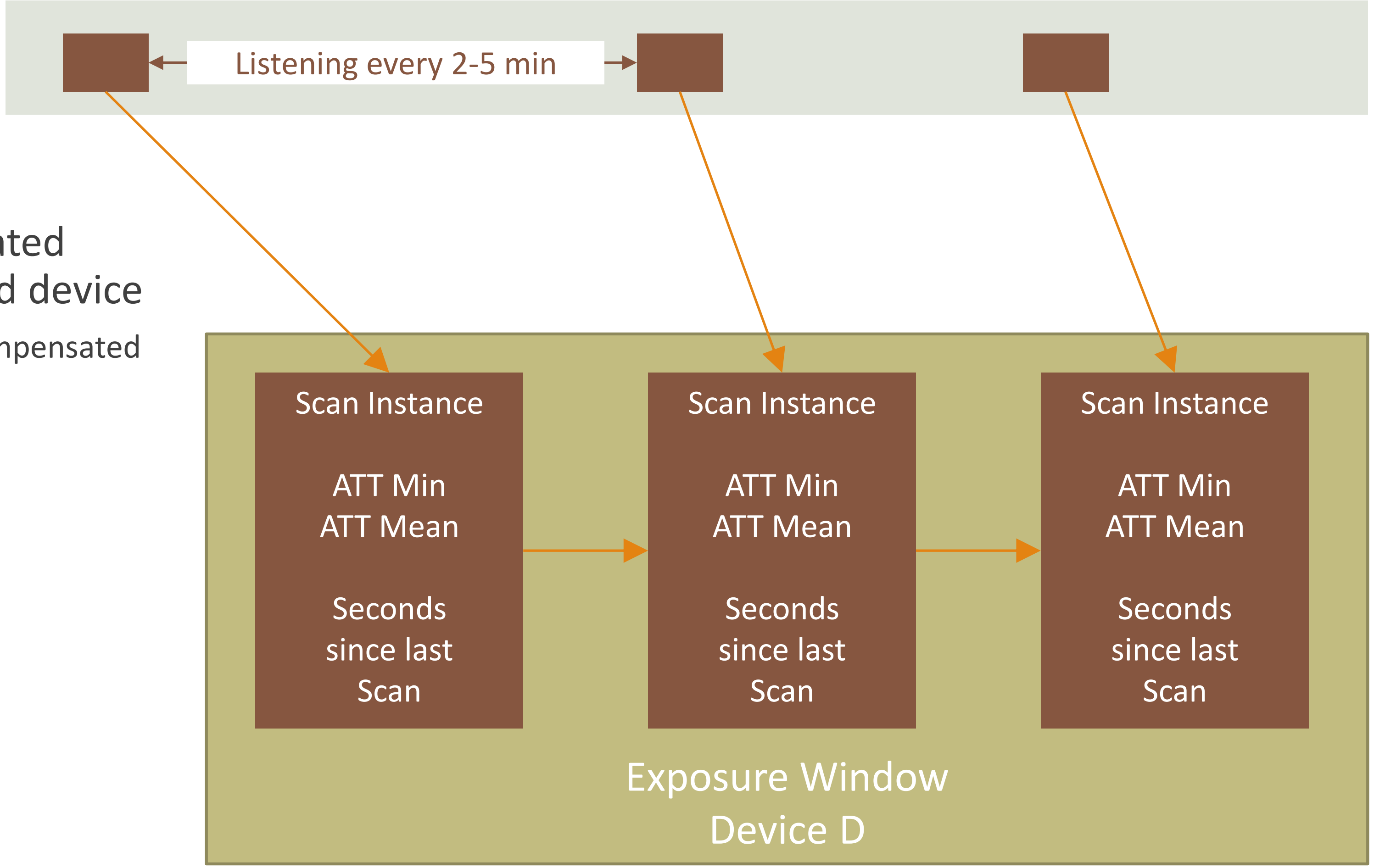
- Reported attenuation (mean, min)
- Time since last listening window



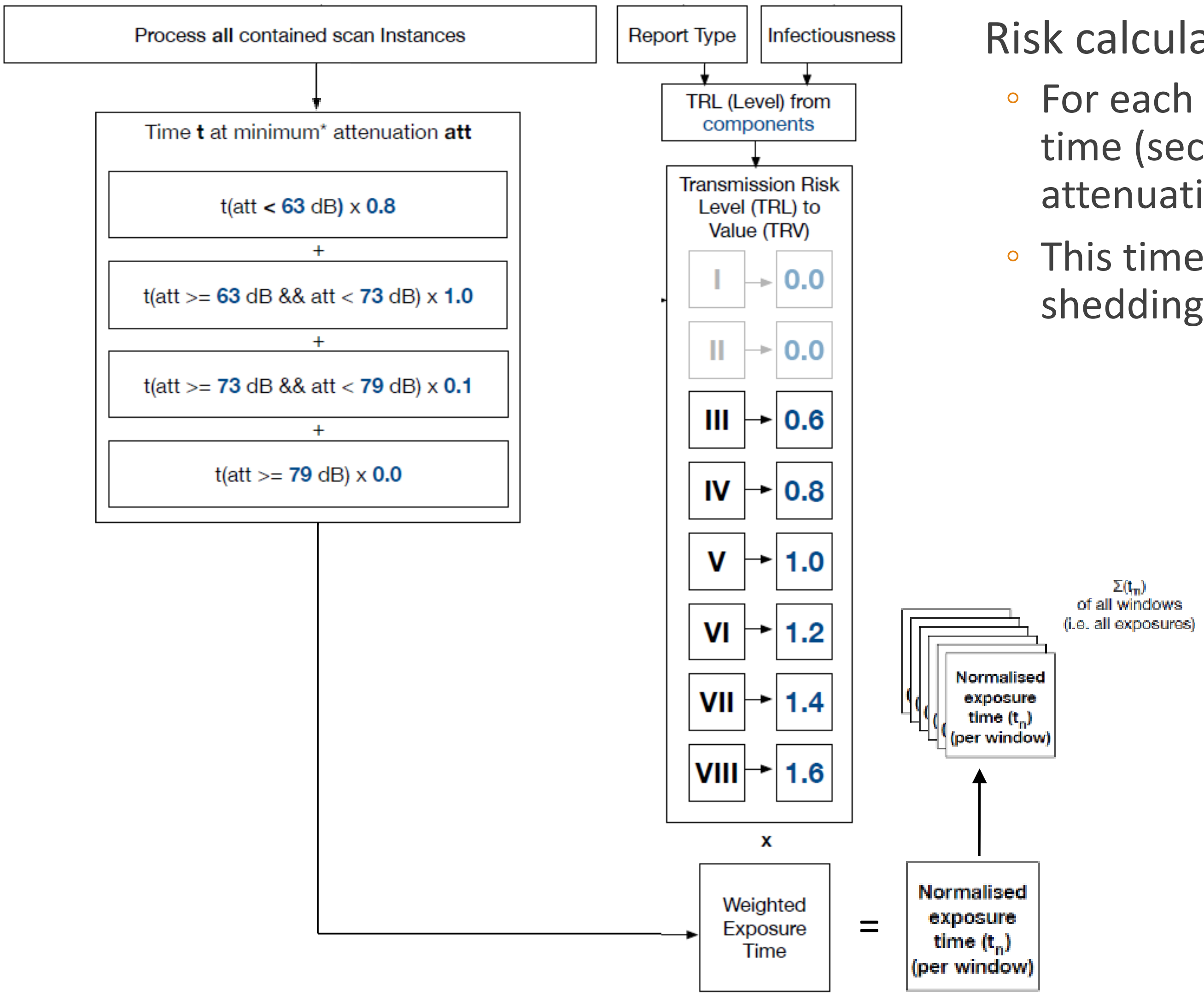
Advanced Features GAEN V2: Exposure Windows

If a device received a diagnosis key (positive tested person) the ENF creates exposure window(s) by submitting this key to the framework.

- Each exposure window contains at least one scan instance (up to 30 min length)
  - Starts counting with the first received beacon
- A scan instance represents the compensated signal strength (attenuation) of the traced device
  - Sending power and received antenna path are compensated by calibration values

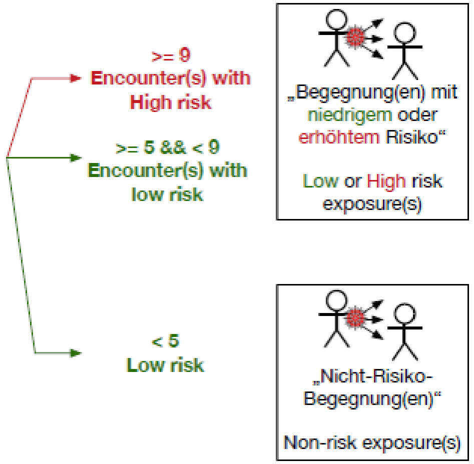


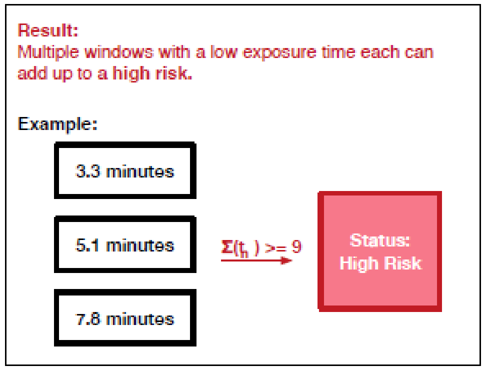
Advanced Features GAEN V2: Risk Calculation



Risk calculation

- For each Scan Instance of the processed Exposure Windows the time (secondsSinceLastScan) are weighed dependent on min attenuation values (buckets) to a weighted exposure time
- This time is normalized by the TRV (simplified: higher virus shedding means height factor)





Source: https://github.com/corona-warn-app/cwa-documentation/blob/main/solution_architecture.md

Real-life implementation: The Corona-Warn-App system

Germany’s official DCT system

- mobile app for Android and iOS devices
- > 45 Mio downloads since June 2020
- > 25 Mio active users at its maximum
- proximity and presence tracing

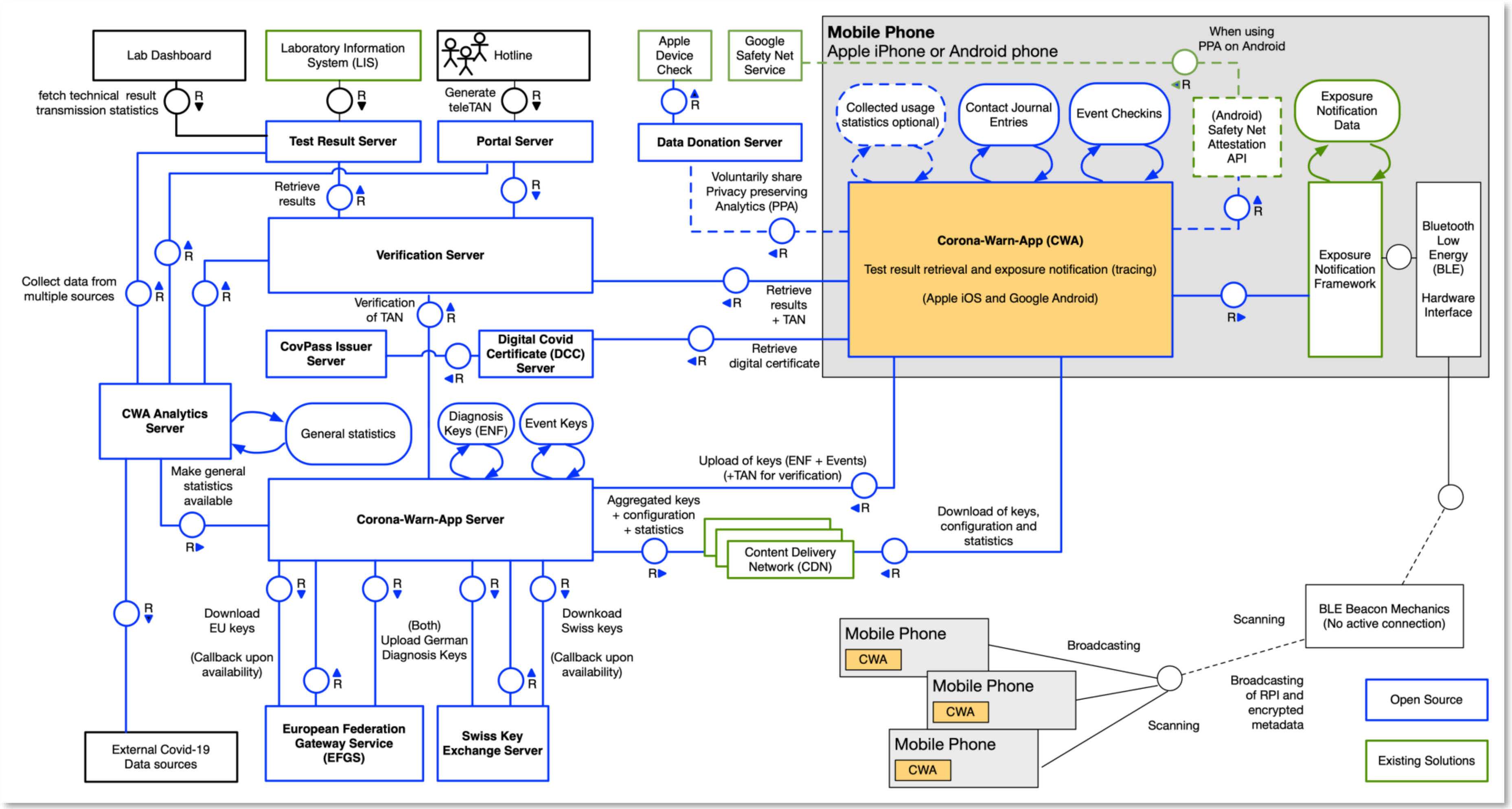
Built on top of GAEN framework (decentral)

Collaboration of several partners

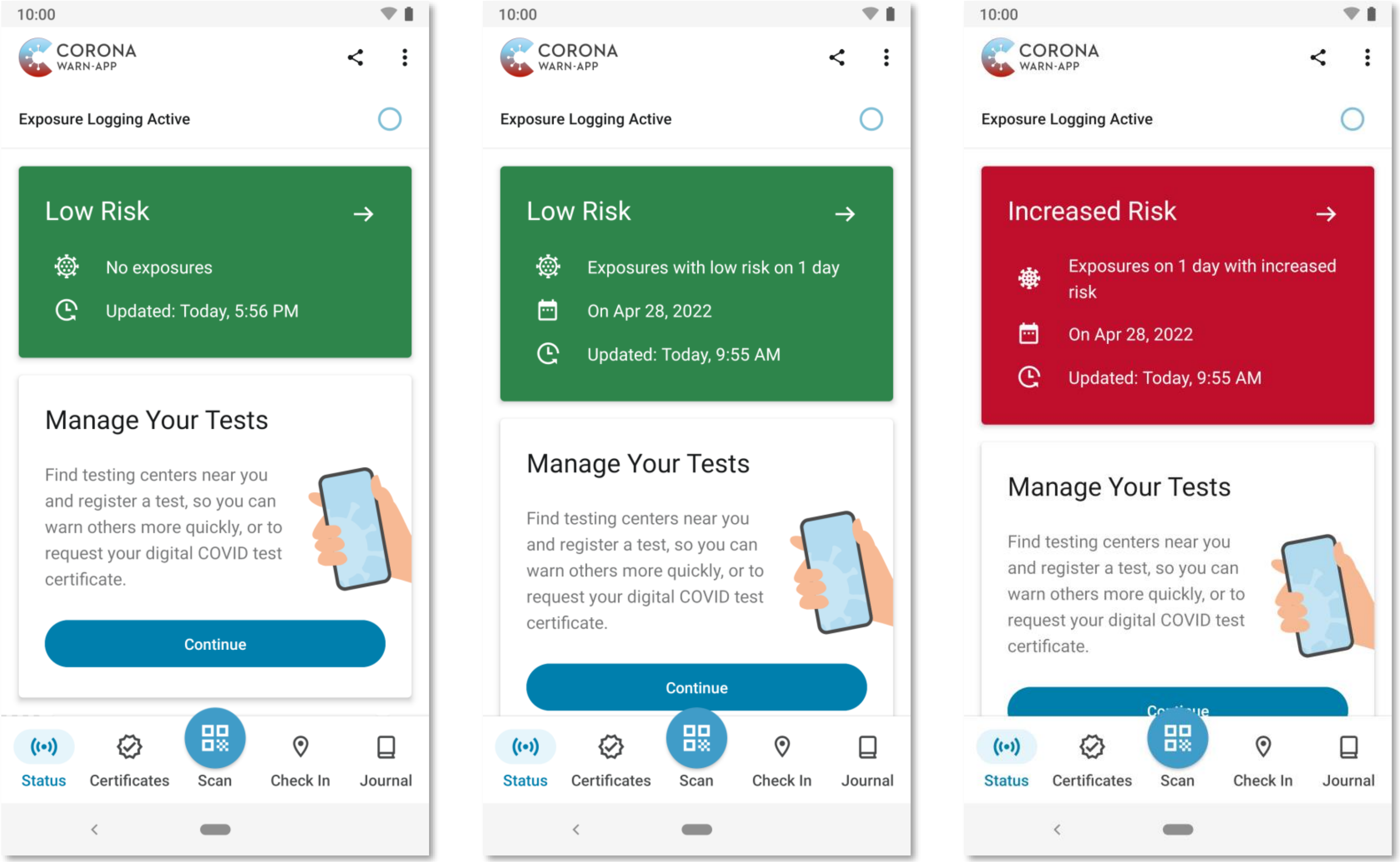
BCG BOSTON CONSULTING GROUP · BCG Digital Ventures · CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY · DETECON CONSULTING · Edelman · Fraunhofer · HealthyTogether · HELMHOLTZ RESEARCH FOR GRAND CHALLENGES · .msg · ROBERT KOCH INSTITUT · SAP · T · · · TÜViT TÜV NORD GROUP

CORONA WARN-APP

Architecture of the Corona-Warn-App System



Corona-Warn-App Notifies Users of Exposures



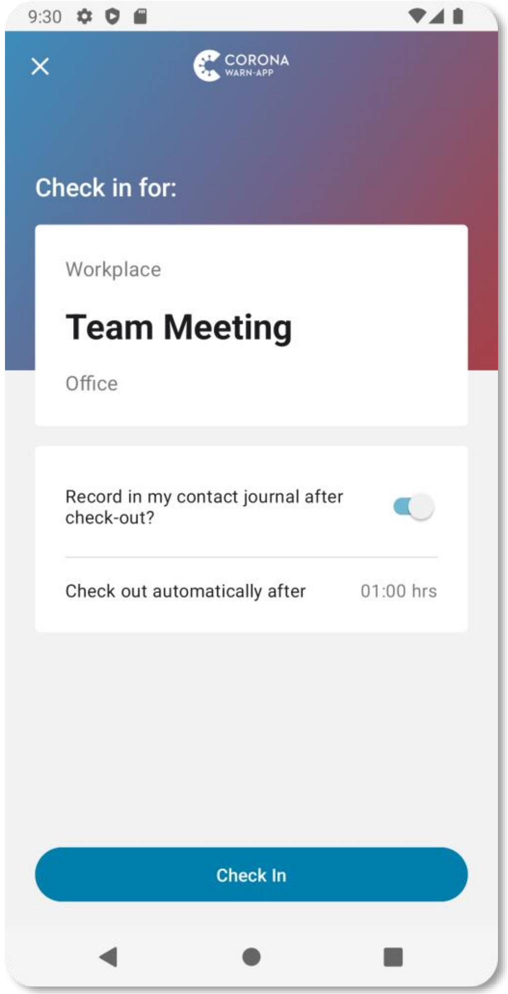
Different risk levels

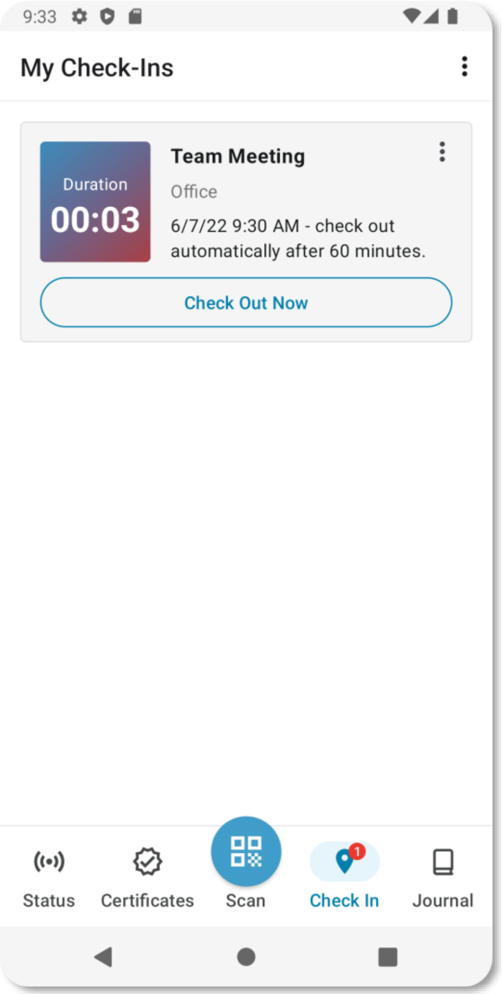
- Low risk without encounter
  - follow the usual recommendations
- Low risk with encounter
  - Encounter was 'too short' or 'too far away'
  - follow the usual recommendations
- High risk
  - get tested

Aggregates different tracing approaches

- proximity tracing
- presence tracing

Presence Tracing - Users Can Check Into Locations and Events





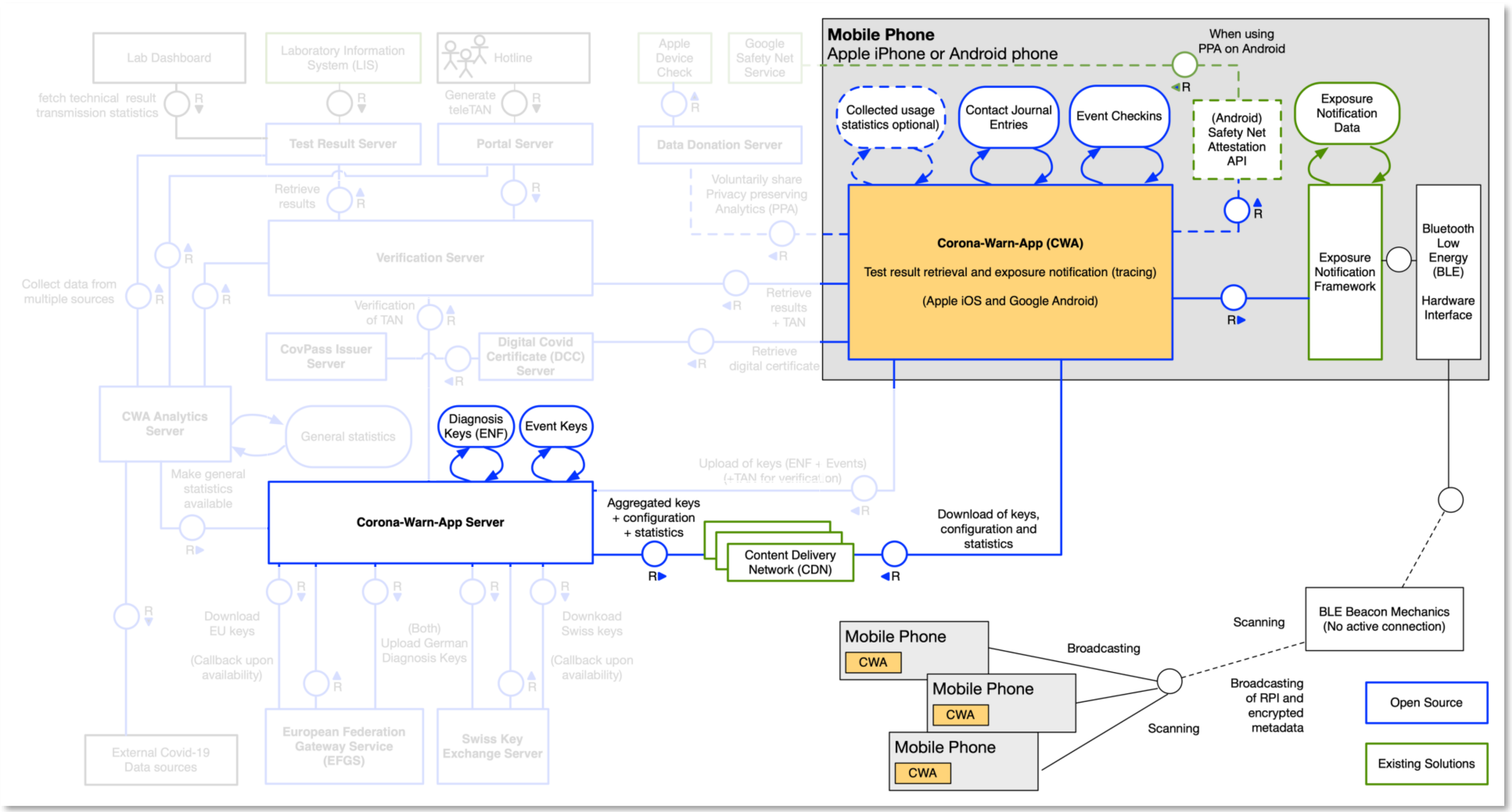
Host perspective (left)

- create QR code for location or event (offline)
- QR code contains metadata (name, location, typical check-in duration, etc.)
- show QR code on phone or print

Attendee perspective (right)

- scan QR code to check in (offline)
- checked out automatically after pre-set time

Architecture of the Corona-Warn-App System



Mobile app

- uses GAEN
- runs on Android/iOS

CWA Server

- distributes TEKs for on-device matching via CDN

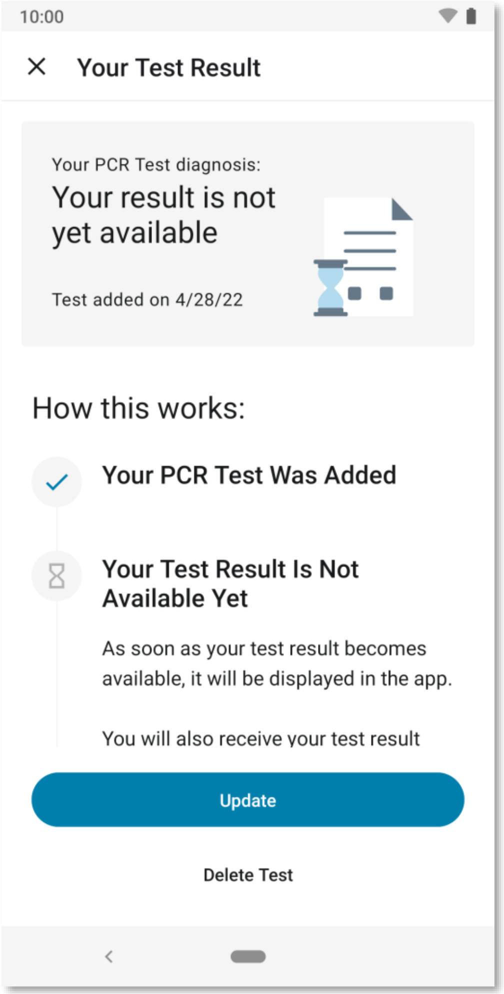
CDN

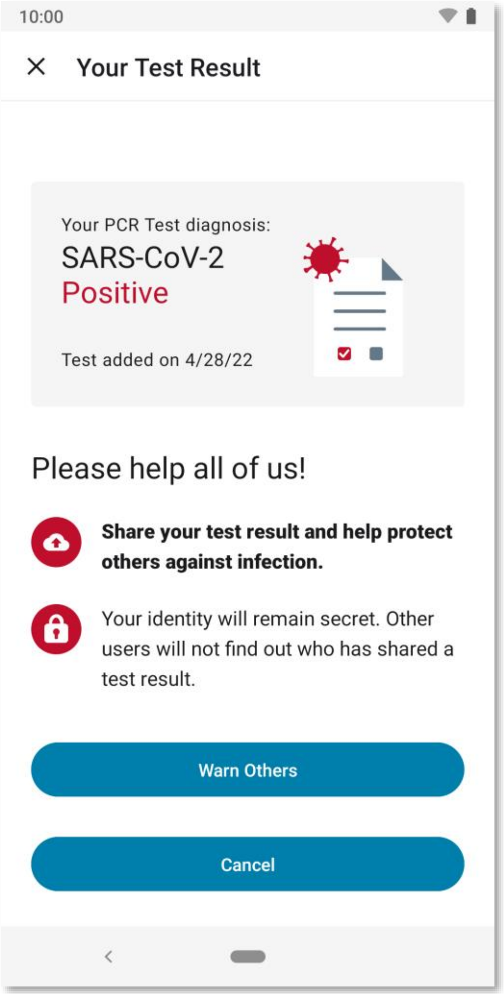
- designed for serving static content
- served 300 TB per day at peak times[1]

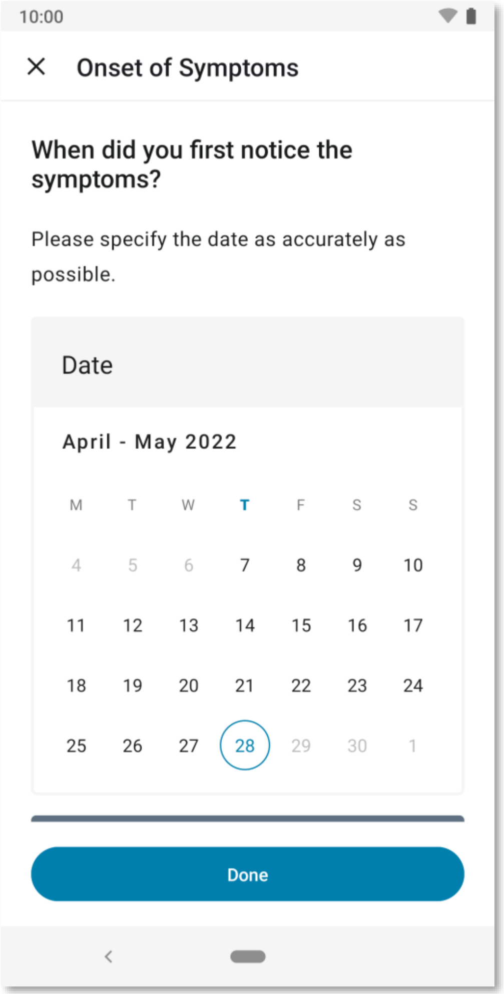
[1] >450k TEKs/day x ~18 Bytes/TEK x 2/device[2] x 20 Mio active devices = ~300TB/day

[2] devices can download TEKs on an hourly basis and additionally on a daily basis; twice in total

Test Registration and Notifying Others via the Corona-Warn-App







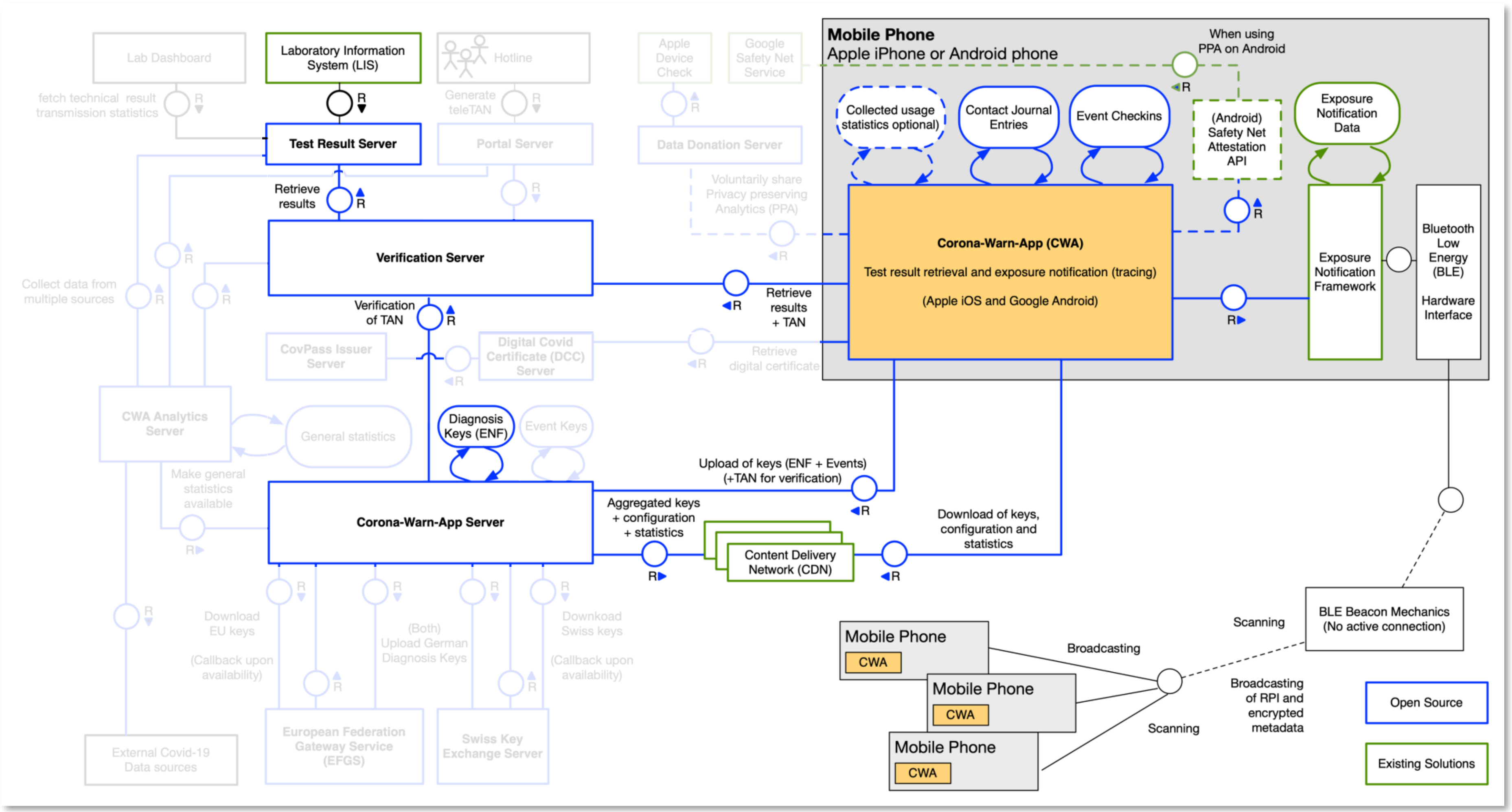
Test registration via QR code

- Support for PCR and rapid antigen tests
- Test result delivered into the app

Notifying Others

- Positive test result allows to warn others
- Onset of symptoms improves accuracy of notification

Architecture of the Corona-Warn-App System



Verification Server

- provides test results to CWA
- restricts registration to one device

Test Result Server

- receives results from labs and rapid antigen test partners

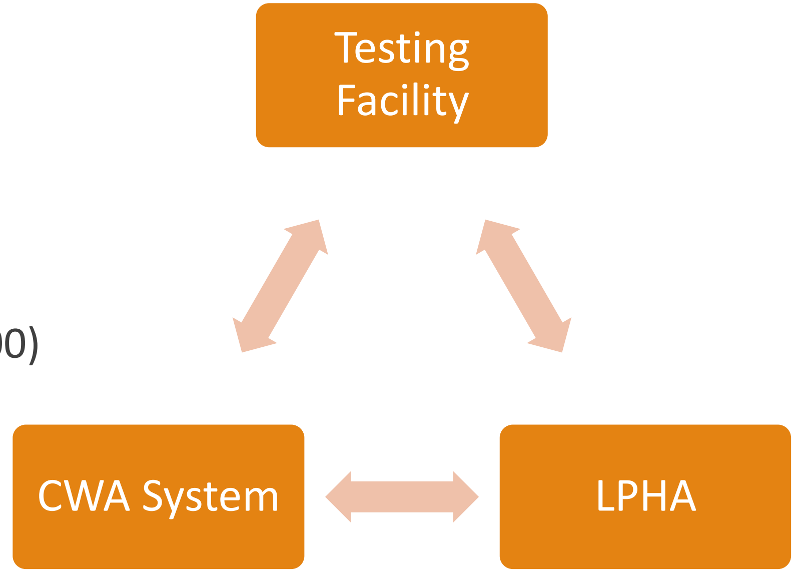
CWA Server

- receives TEKs and one-time upload TAN
- verifies TAN against Verification Server

Real-life implementation: The Corona-Warn-App system

Integration with testing facilities and local public health authorities

1. Testing
- Strong proliferation of testing facilities (Bürgertest = “Citizens’ test”), 10,000+
- Legal requirement to be connected to the Corona-Warn-App backend
  - test type, result
- Legal requirement of disease notification to the local public health authority (~400)
  - test type, result (pos. only), testing facility, data on tested person
- Integration with app
  - test registration
  - rapid test profile
  - results pulled from lab result server
  - automatically validated for key upload
- LPHA will contact notified person (phone call, letter)
  - issues isolation order
  - gives recommendations
  - conducts conventional/manual contact tracing
  - will not know about use of Corona-Warn-App



Unfortunately, no integration between Corona Warn App system and disease notification system regarding data flow from testing facilities

Real-life implementation: The Corona-Warn-App system

Integration with local public health authorities

CWA System ⟷ LPHA

2. Contact Tracing

- Different focus, different strengths
  - **informal contact tracing** -> people you are well connected to (friends and family)
  - **conventional contact tracing** -> other people that can be identified (by yourself or with your help)
  - **digital contact tracing** -> people you cannot identify (lack of knowledge), you may not have noticed (lack of attention), or you may have forgotten (lack of memory)
- Weak integration between app and local public health authority
  - person warned by app (exposure notification) not known to LPHA
  - may decide to contact LPHA (no app feature)
  - may request quarantine order (no app feature)
  - can share contact diary contents with LPHA (app feature)
- LPHA may contact notified person (phone call, letter)
  - issues quarantine order
  - gives recommendations
  - will not know about use of Corona-Warn-App

Scalability

- informal contact tracing scales automatically
- digital contact tracing can easily be scaled
- conventional contact tracing is difficult to scale
  - at low incidence (early in the pandemic) LPHAs would try to find all contact persons
  - later they would only try to reach out to contact persons with readily available contact information
  - finally they would give up and leave it to informal and digital contact tracing -> thus need for
    - better and customized recommendations
    - automated quarantine orders

System Architecture
CWA Exposure Estimation and Parameters

CWA groups encounters with COVID-19 positive people reported by GAEN into four attenuation buckets:

Near [0, a_N) [dB]	**Mid** [a_N, a_M) [dB]	**Far** [a_M, a_F) [dB]	**Very Far** [a_F, ∞) [dB]
Time in Near [min]	Time in Mid [min]	Time in Far [min]	Time in Very Far [min]

Buckets contain total time of exposure in this attenuation range in a 30 min time window.

Exposure Score is calculated by weighted sum:

$$\mathrm{ES} = w_n \cdot t_n + w_m \cdot t_m + w_f \cdot t_f + w_{vf} \cdot t_{vf}$$

ES: Exposure Score (minutes)
w_x: Weight for near, mid, far, very far
t_x: Time (minutes) in near, mid, far, very far

If ES is exceeding a threshold of 9 minutes (in one day) a warning will be displayed.

System Architecture
CWA Exposure Estimation vs. Epidemiological Risk Model

CWA Exposure Estimation	**Epidemiological Risk Model (RKI)**
Four attenuation classes: near, mid, far, very far $[0, a_N), [a_N, a_M), [a_M, a_F), [a_F, \infty)$	Two distance classes: risky, not risky $[0m, 1.5m), [1.5m, \infty)$
Exposure Score calculation: $ES = w_n \cdot t_n + w_m \cdot t_m + w_f \cdot t_f + w_{vf} \cdot t_{vf}$ w_n, w_m, w_f, w_{vf}	Exposure Score calculation: $ES_{EPI} = t_{risky}$
Threshold for warning: $ES >= T$ T	Threshold for warning: $ES_{EPI} >= T_{EPI}$ $T_{EPI} = 10$ min

Testing and parameters optimization

Goal: Fit CWA Exposure Estimation to Epidemiological Model

Basic assumption:

- Epidemiological Model of RKI is considered as Ground Truth

Steps:

- Set up experiments in relevant settings
- Record Data about distances, attenuations and durations

Evaluate fitting of CWA results to Epidemiological Model for different parameters:

- *Will CWA issue warnings according to the Epidemiological Model?*
- Enhance CWA Model Parameters

CWA Exposure Estimation	Epidemiological Risk Model (RKI)
Four attenuation classes: near, mid, far, very far $[0, a_N), [a_N, a_M), [a_M, a_F), [a_F, \infty)$	Two distance classes: risky, not risky $[0m, 1.5m), [1.5m, \infty)$
Exposure Score calculation: $ES = w_n \cdot t_n + w_m \cdot t_m + w_f \cdot t_f + w_{vf} \cdot t_{vf}$ w_n, w_m, w_f, w_{vf}	Exposure Score calculation: $ES_{EPI} = t_{risky}$
Threshold for warning: ES >= T T	Threshold for warning: $ES_{EPI} >= T_{EPI}$ $T_{EPI} = 10$ min
CWA Results	Ground Truth

Experiments
Metric and Optimization Goal 1/2

Metric for Fitting:

$$F_\beta = (1+\beta^2)\cdot\frac{precision \cdot recall}{(\beta^2 \cdot precision) + recall} = \frac{(1+\beta^2)\cdot TP}{(1+\beta^2)\cdot TP + \beta^2 \cdot FN + FP}.$$

F_2 will result in:

Low number of FN
(low number of undetected risky contacts)

Medium number of FP
(extra COVID-testing capacity needed)

Confusion Matrix

CWA Results	Risky Contact (Exposure)	Not Risky Contact (No Exposure)
Warning (Exposure)	True Positives (TP)	False Positives (FP)
No Warning (No Exposure)	False Negatives (FN)	True Negatives (TN)

Ground Truth
(Epidemiological Model)

Experiments
Metric and Optimization Goal 2/2

Advanced Metric for μ3‘ Fitting:

$$\mu 3' = \frac{2}{3} \cdot MCC3 + \frac{1}{3} \cdot \tilde{F}$$

$$MCC_3 = \frac{C \cdot S - r \cdot R - g \cdot G - n \cdot N}{\sqrt{S^2 - r^2 - g^2 - n^2} \cdot \sqrt{S^2 - R^2 - G^2 - N^2}}$$

$$\begin{aligned} C &= rR + gG + nN \\ r &= rR + rG + rN \\ g &= gR + gG + gN \\ n &= nR + nG + nN \\ R &= rR + gR + nR \\ G &= rG + gG + nG \\ N &= rN + gN + nN \\ S &= rR + rG + rN + gR + gG + gN + nR + nG + nN \\ &= r + g + n \\ &= R + G + N \end{aligned}$$

$$\tilde{F} = \frac{6 \cdot rR + 3 \cdot gG}{6 \cdot rR + 3 \cdot gG + 1 \cdot rG + 3 \cdot rN + 3 \cdot gR + 2 \cdot gN + 6 \cdot nR + 3 \cdot nG}$$

3x3 Confusion Matrix

Rows: CWA Results; Columns: Ground Truth (Epidemiological Model)

	Class	R	G	N	Sum
Red Warnings (**r**ed Exposure)	r	rR	rG	rN	r
Green Warnings (**g**reen Exposure)	g	gR	gG	gN	g
No Warning (**n**o Exposure)	n	nR	nG	nN	n
	Sum	R	G	N	S
		High risky Contact (**R**ed Exposure)	Minor risky Contact (**G**reen Exposure)	Low Risky Contact (**N**o Exposure)	

Ground Truth
(Epidemiological Model)

The Metric μ3‘:

1. MCC_3 favors right classifaction
2. F̃ favors „too many warnings“ over „too few warnings“
3. μ3‘ combines both approaches

Experiments
Hardware and Software Infrastructure

Phones and Software:

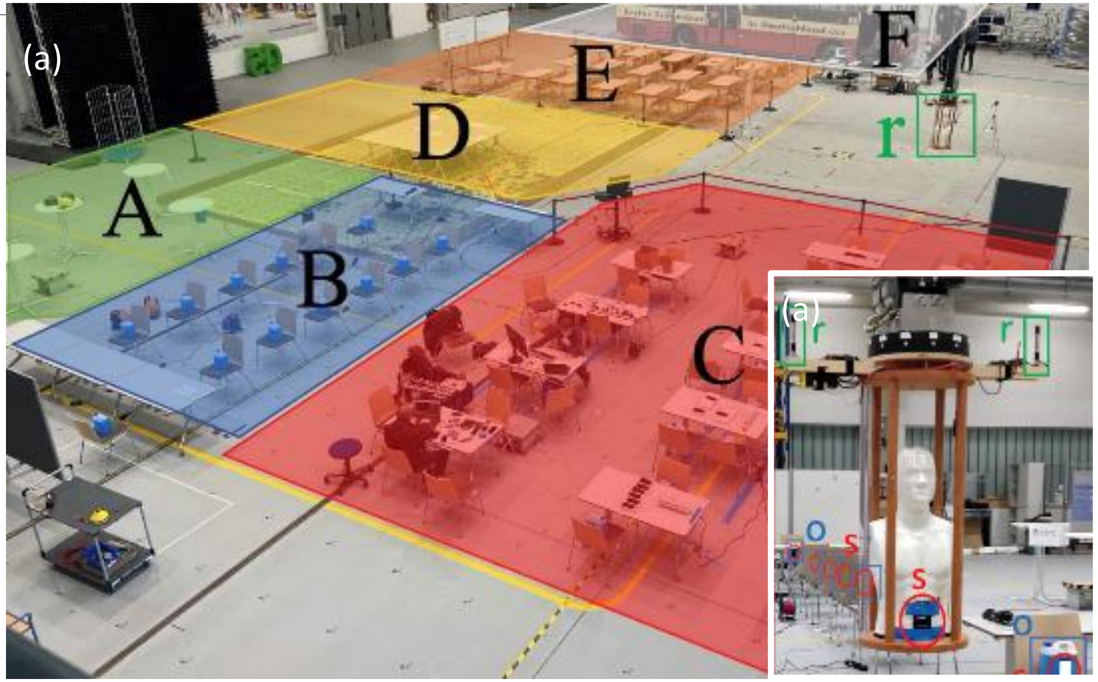
- 40 Android Phones with modified CWA App (Auto Start/Stop/Reset and logging debug data)
- Raspberry Pis for scripted setup and testing

Controlled Synthetic Experiments at LINK Center (a):

- (automated) 3D Crane system with Body Double
- Nikon iGPS Reference Positioning ($CEP_{95} < 0.9$ cm)

Semi-controlled Real-world Experiments (b):

- Participants carring Smartphones
- Qualisys Camera-based (mobile) Reference Positioning ($CEP_{95} < 1$ cm)

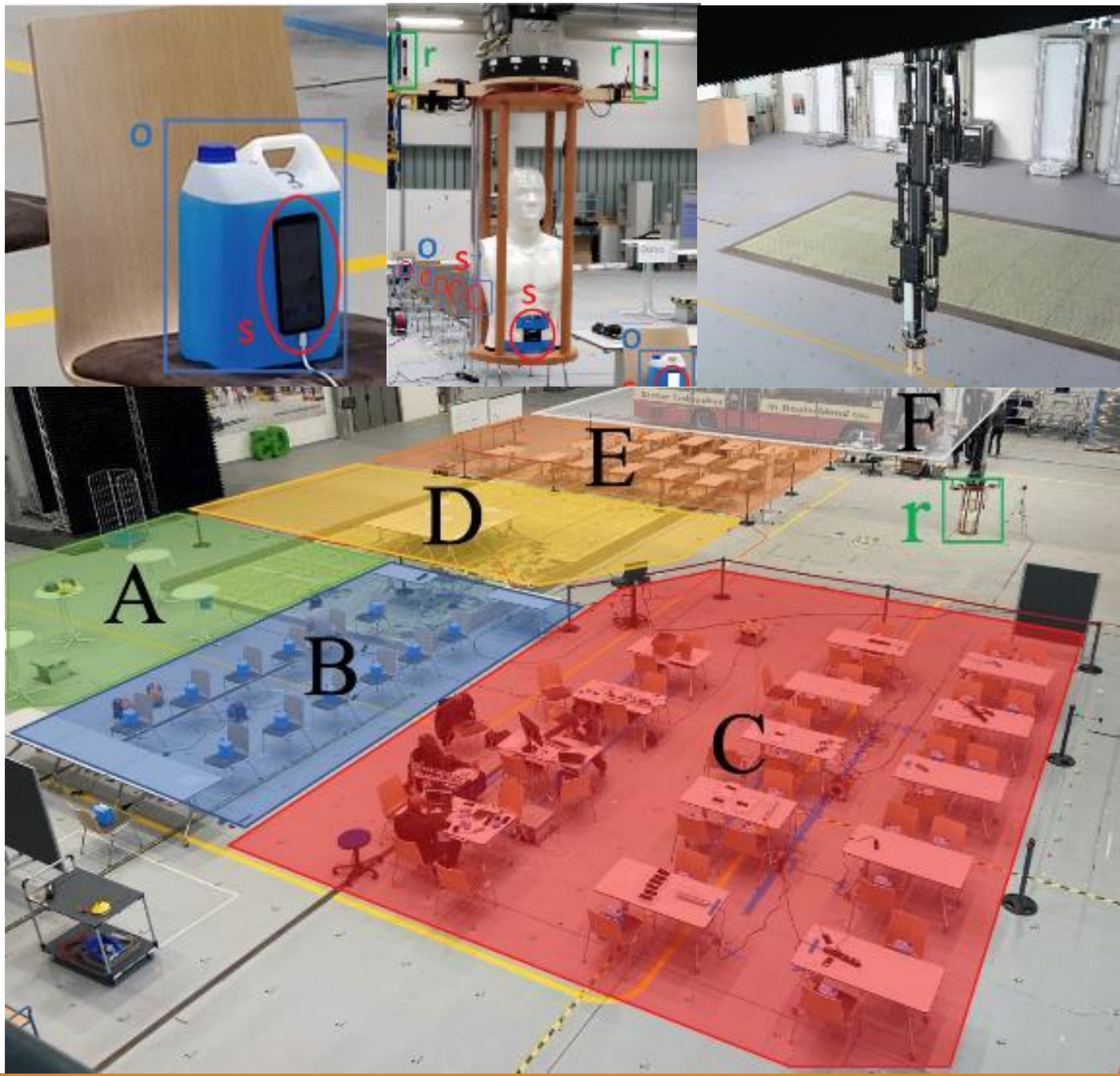


Experiments

Controlled Synthetic Experiments

Fully automated 3D Positioning System simulates different scenarios:

- **Bar (A):** People standing at tables, moving waiter (r)
- **Queue (D):** Typical queuing situation, person (r) e.g., a cash register with 2 queues
- **Dining Restaurant (C):** 14 tables with guests and a waiter (r)
- **Fairground (A-E):** Visitor (r) moving through exhibition
- **Fast Food Restaurant (B, C):** Guest (r) queuing at service desk, then taking seat
- **Large Office (A-D):** Employee (r) working at desk, moves to printer room, visits collegues, moves to meeting room
- **School (E):** teacher (r) writes at board, then moves through classroom
- **Crowd (D):** Person (r) moves randomly in the middle or around a crowd
- **Shopping Center (A-E):** Person (r) moves naturally within a crowd and waits at random places for vairous periods of time



Experiments

Controlled Synthetic Experiments - Video

VIDEO1

Experiments

Semi-Controlled Real-world Experiments

Participants play real-world scenes in real-world settings:

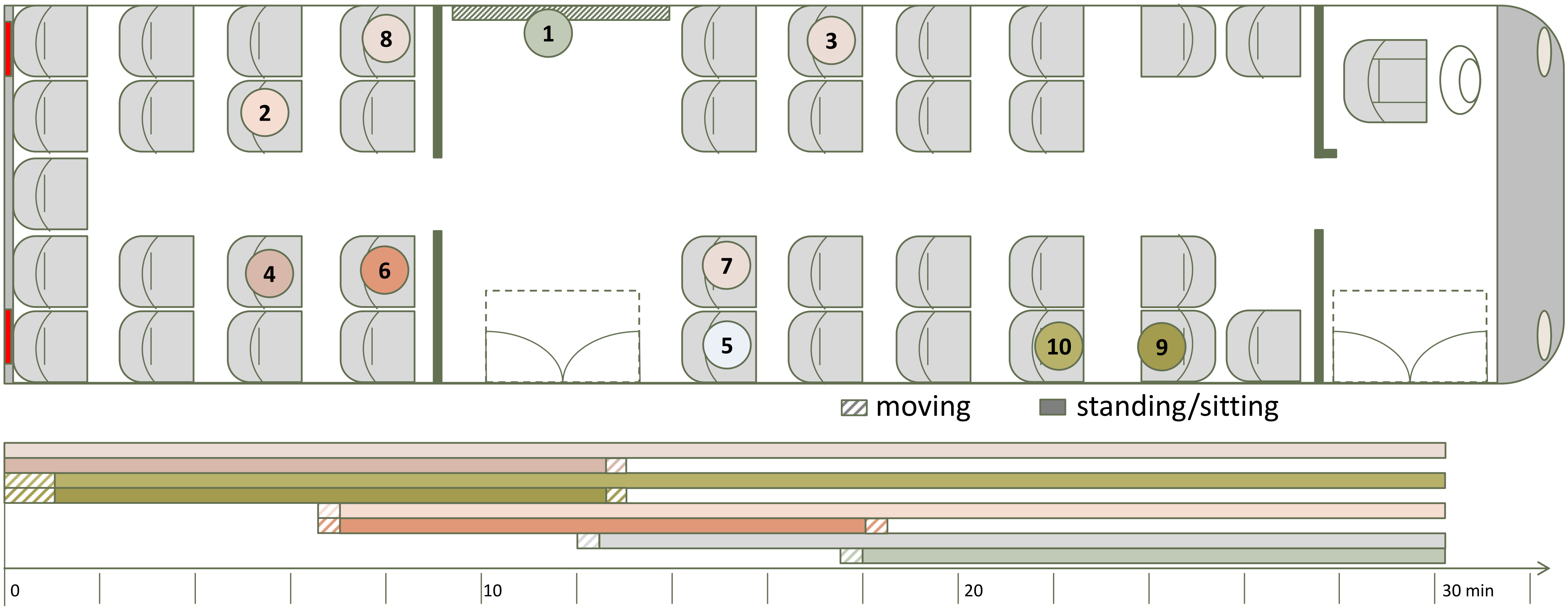
- Vehicles: Bus, Underground, Airplane, 10-20 Participants with smartphones
- helmets for optical reference positioning

Scenarios

- Public Bus:
  Getting in/out and switching line and variing seat placements
- Underground:
  Getting in/out, again variiring seat placements
- Plane:
  typical seating, boarding, unboarding, in-flight service and using toilets


Experiments

Bus Test Design: Example



Experiments
Semi-Controlled Real-world Experiments

Controlled Synthetic Experiments - Video

VIDEO2

Results

General Results for Optimal Parameters (µ3' Metric)

Some numbers:

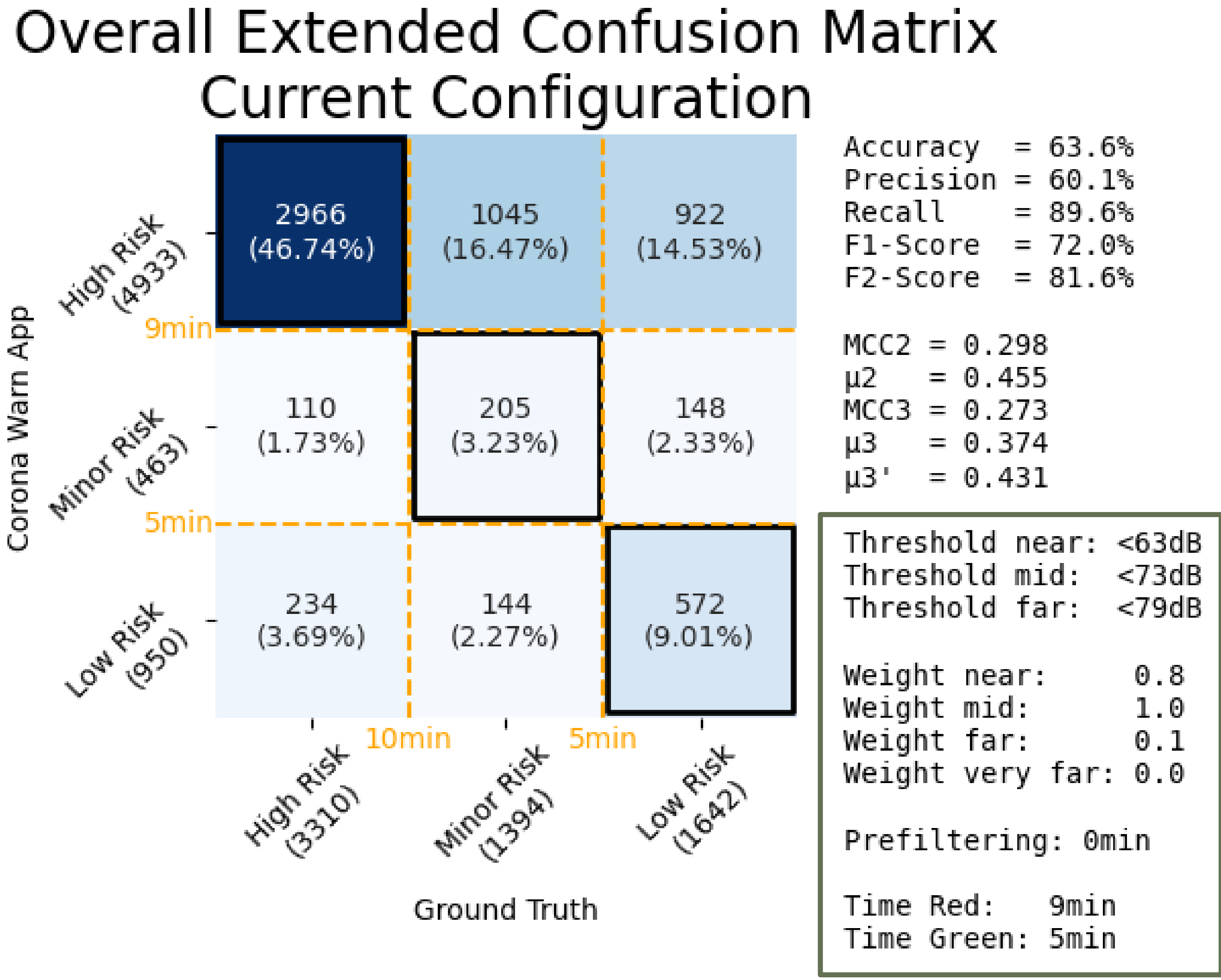
- 6,346 measured contacts: (4,680 in controlled synthetic, 1,666 in semi-controlled real-world) 8,313 minutes total testing time
- ~3 weeks of 3D Positioning System (Crane) Movement

General Results:

- Large number of parameter constellations that show acceptable µ3' results
- Low Number of False Negatives (Minor and low risk CWA by High risk GT)
- High Number of False Positives (Minor and low risk GT by High risk CWA)

Unexpected Detail:

- Optimal „Weight near“ is lower than „Weight mid“



Results
Scenario Specific Results (F_2 Metric)

Results:

- Results are highly scenario depended.
- Results are influenced by:
  - Scenario specific exposure times
  - Phone position
  - Dynamic in scenarios (People movement)
  - Shadowing in crowds
  - Signal propagation in metal tubes
- Scenario-specific parameters can reduce #FN and #FP.
- μ3’ Metric shows similar Scenario specifics

	Controlled									Semi-controlled		
	Bar (A)	Queue (B)	Dining rest. (B+C)	Fairground (A-E)	Fast-food rest. (B+C)	Large office (A-D)	School (E)	Crowd (D)	Shopping center (A-E)	Bus	Airplane	Subway
$\varnothing F_2$	0.88	0.66	0.88	0.58	0.61	0.66	0.68	0.82	0.9	0.86	0.88	0.69
TP	239	104	173	59	95	23	44	670	744	361	275	195
FP	70	181	21	68	72	31	103	377	408	126	181	420
FN	25	23	25	36	59	7	0	88	0	40	0	2
TN	14	148	15	227	152	89	129	161	0	67	0	84

Findings

We presented an extensive measurement campaign that was carried out together with SAP and T-Systems under the supervision of the RKI.

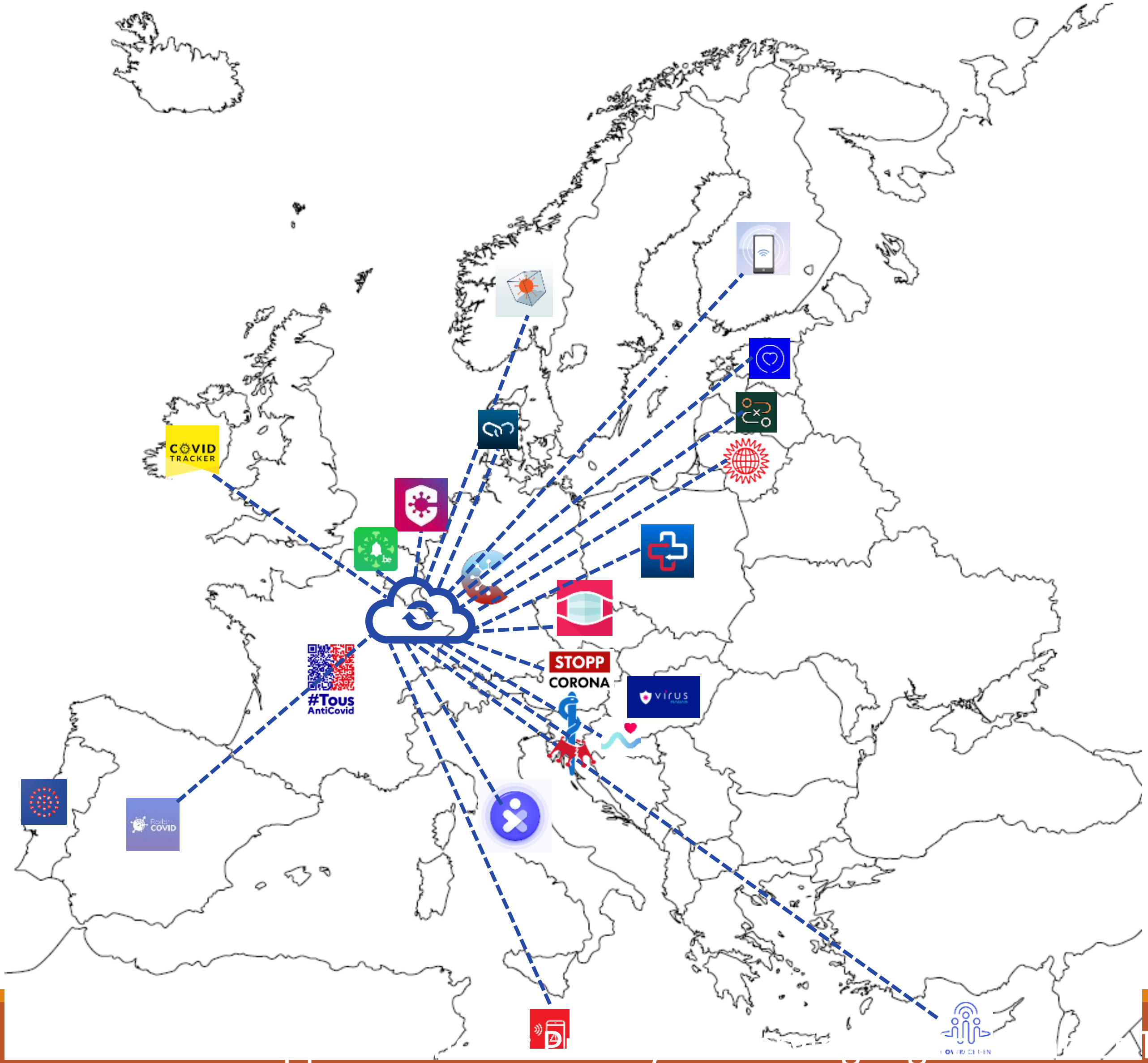
Parameters for decentralized CT (CWA in Germany) have been derived.

Scenario-specific parameters would yield best results.

However, our optimized general parameters show only few false negatives.

Some scenarios where people stay together closely may attenuate or reflect the signals such that contacts are not detected.

Interoperability of MCTA Across Europe



Why not a single pan-European MCTA?

- Allow State-specific integration with national public health system/processes

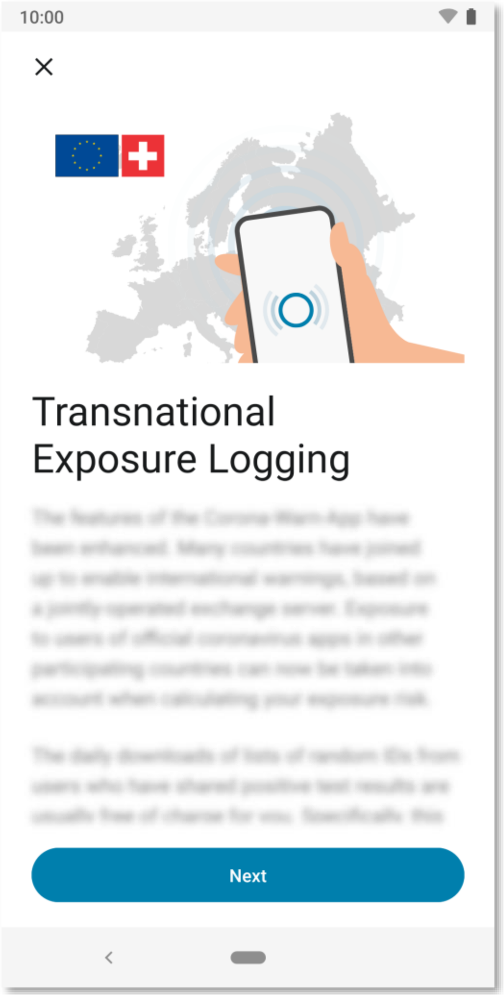
What happens when EU citizens start traveling across Europe?

- The European Federation Gateway Service (EFGS) enables cross-border interoperability
- “Roaming” service for MCTA in Europe

19 EU Member States with GAEN-based MCTA have been connected to the EFGS

- Centralized MCTA (FR, HU) cannot be connected to the EFGS
- 6 MCTA were disconnected (CZ, AT, PL, CY, DK, and EE) by May 2022

Cross-border app interoperability through the European Federation Gateway Service

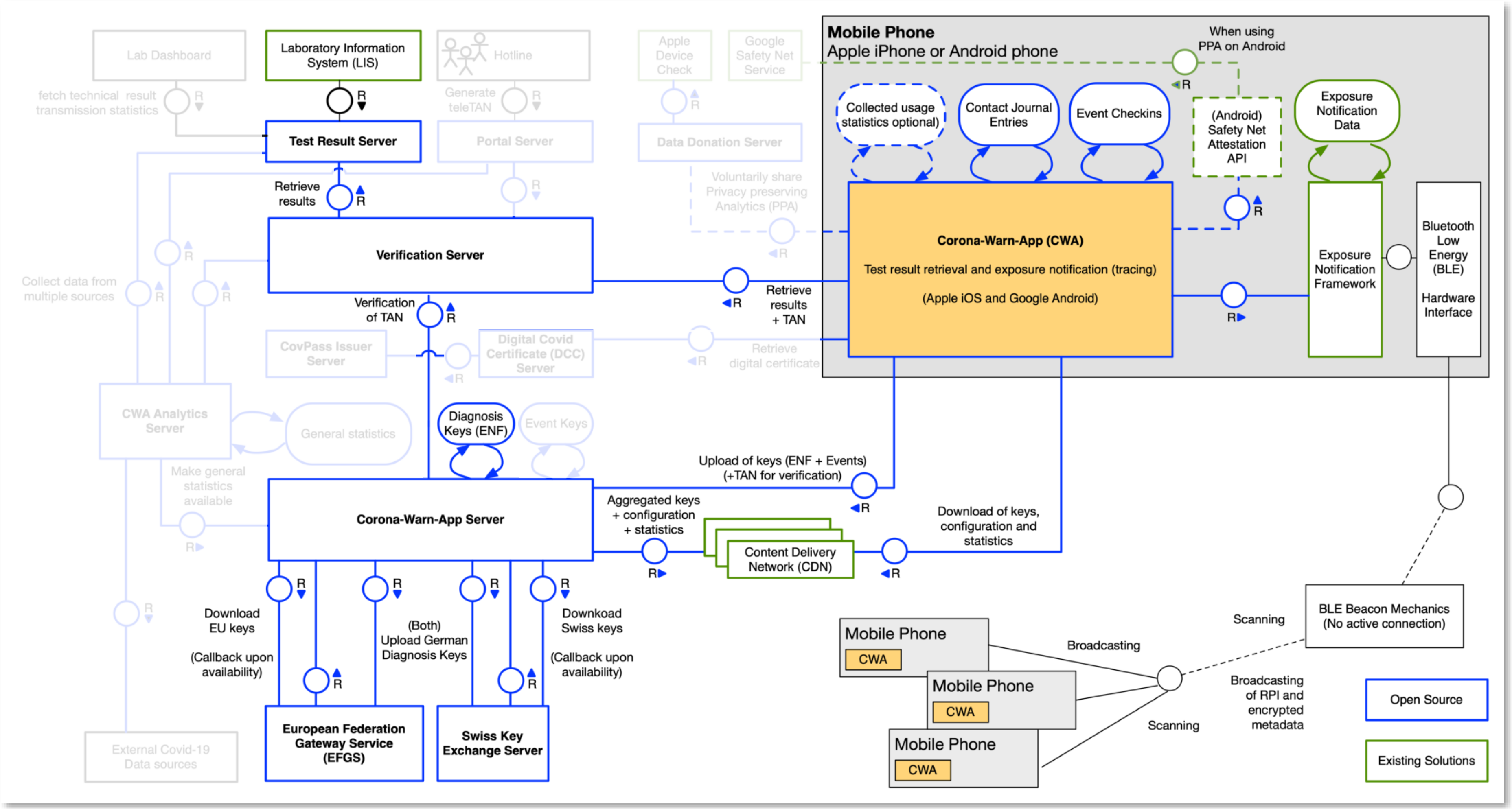


Goal: facilitate notifications across GAEN apps

Sample use case:

- Gerhard from Germany uses CWA
- Bella from Belgium uses her respective DCT app
- they sit next to each other on the bus
- if either one gets infected, the other one should be notified

Architecture for Interoperability



Mobile app

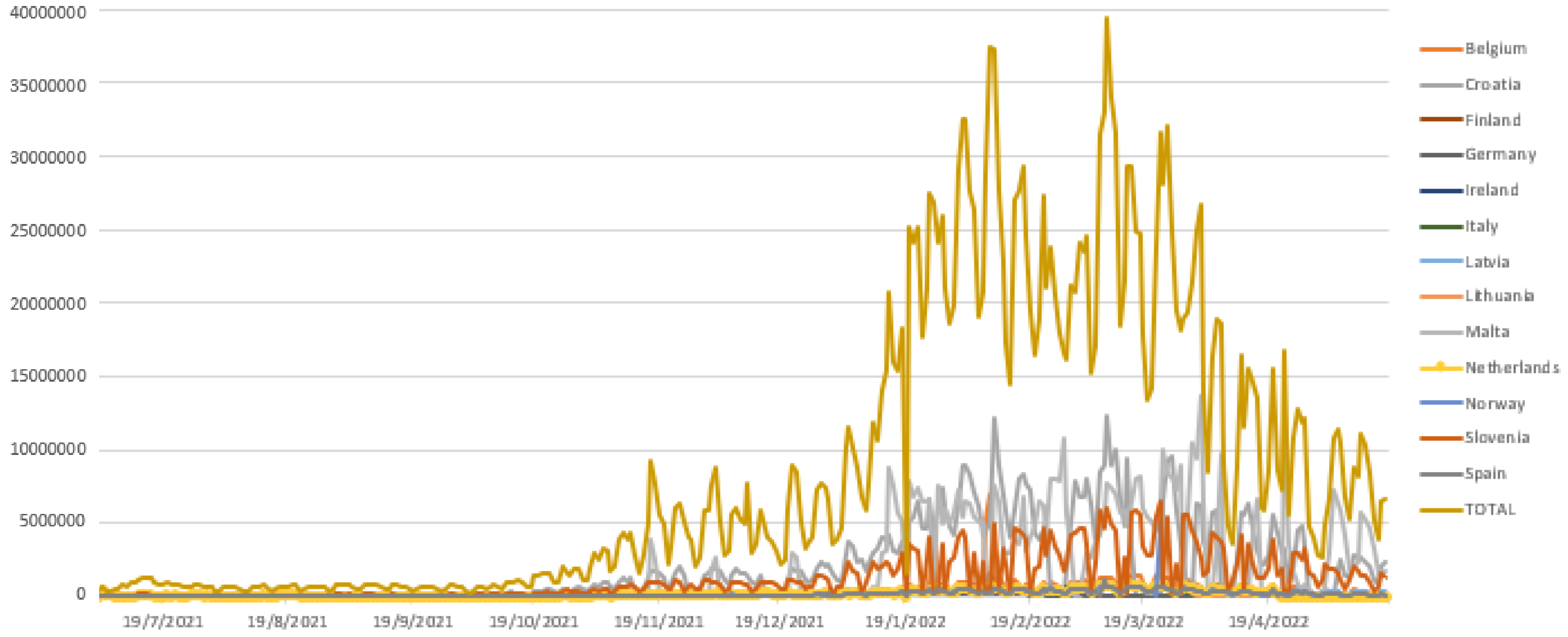
- consent includes sharing TEKs with participating countries
- no country selection; keys are shared with all participants

CWA Server

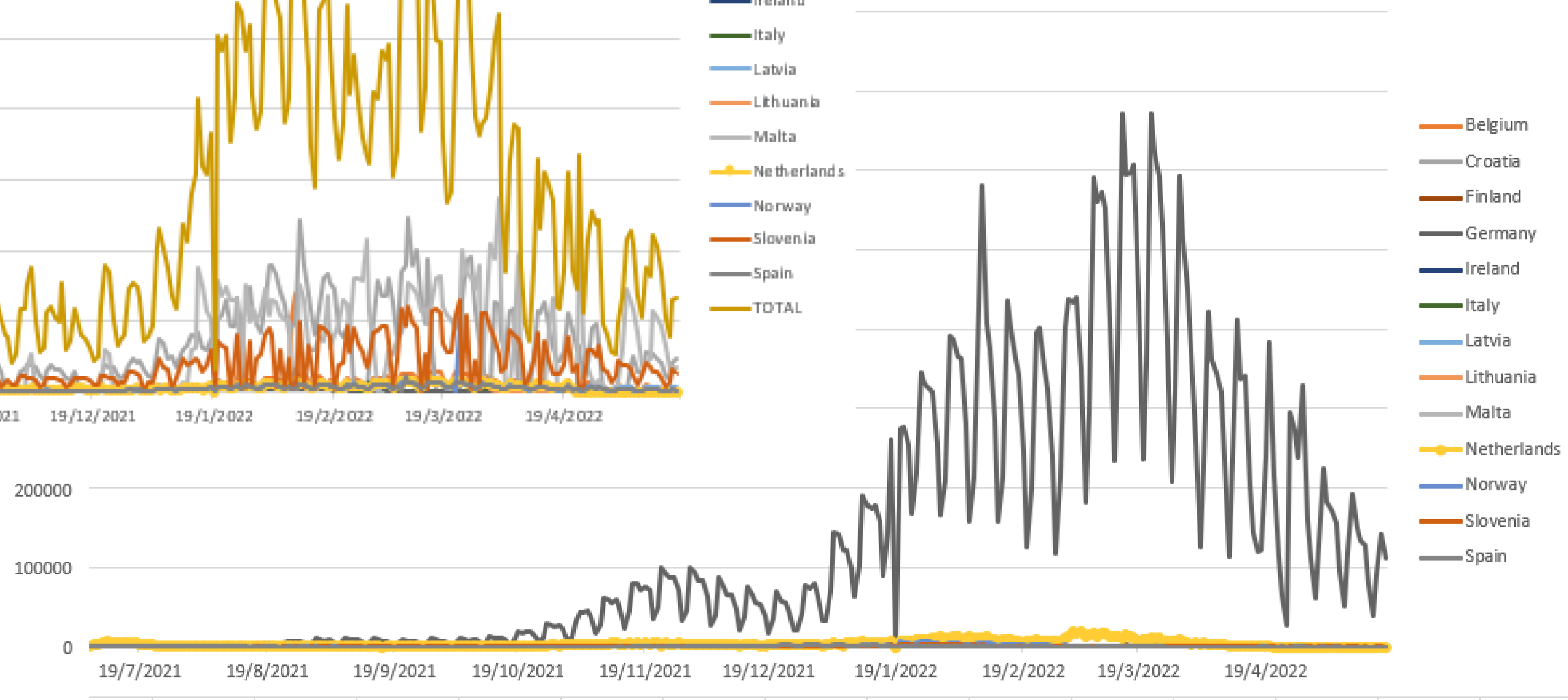
- forwards uploaded TEKs from CWA to EFGS
- downloads foreign TEKs and distributes them with domestic keys via CDN

Keys uploaded/downloaded from/to CWA to/from the EFGS over time

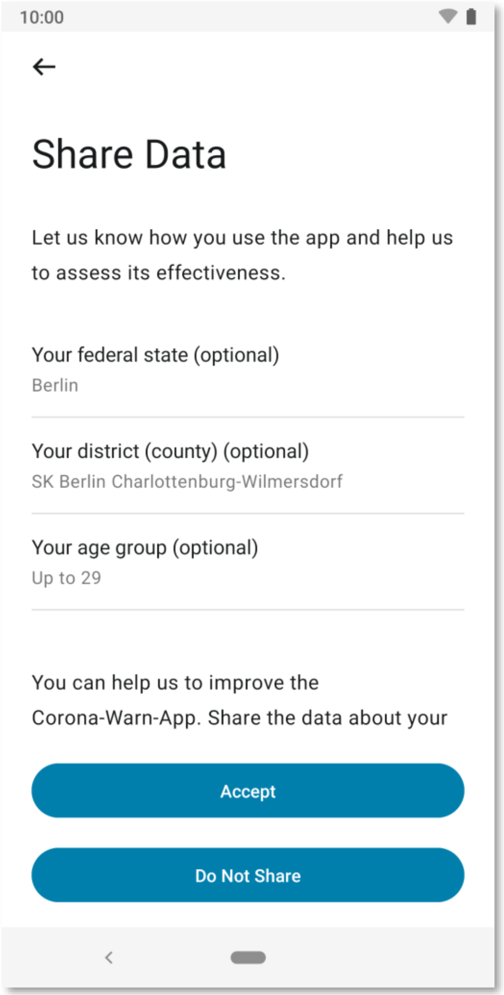
Downloaded (daily)



Uploaded (daily)



Implementation and Integration of Event-Driven User Survey (EDUS) and Privacy-Preserving Analytics (PPA)



Goal: optionally collect usage data while maintaining user's privacy

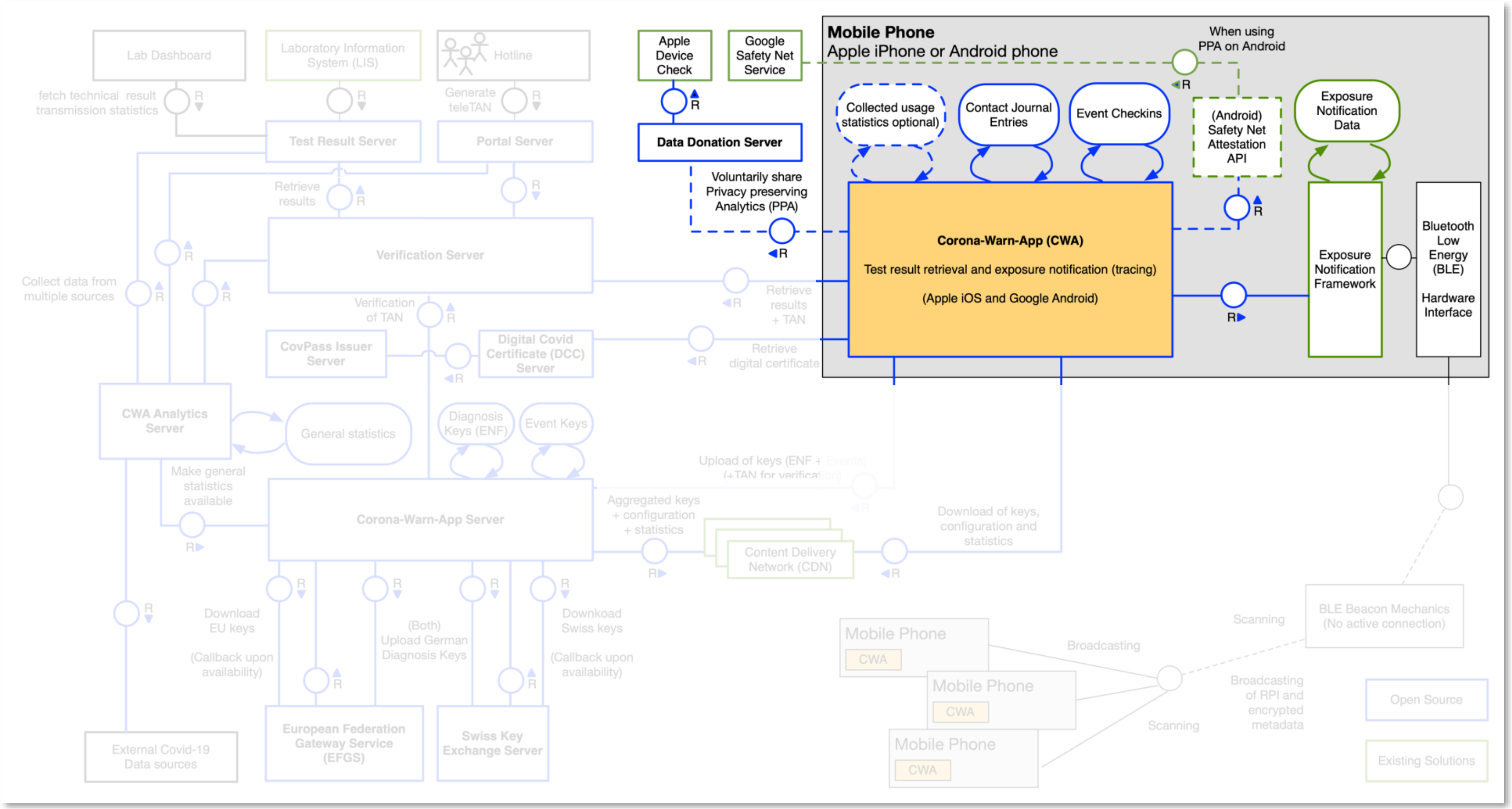
Privacy-preserving Analytics (PPA)

- submitted once per day per participating device
- includes user metadata (e.g. federal state, age group)
- includes client metadata (e.g. app version, operating system, GAEN version)
- includes metrics
- > 10 Mio device donate daily

Event-driven User Survey (EDUS)

- allow for survey participation when a 'high risk' encounter is received

Architecture of PPA and EDUS for Android Devices



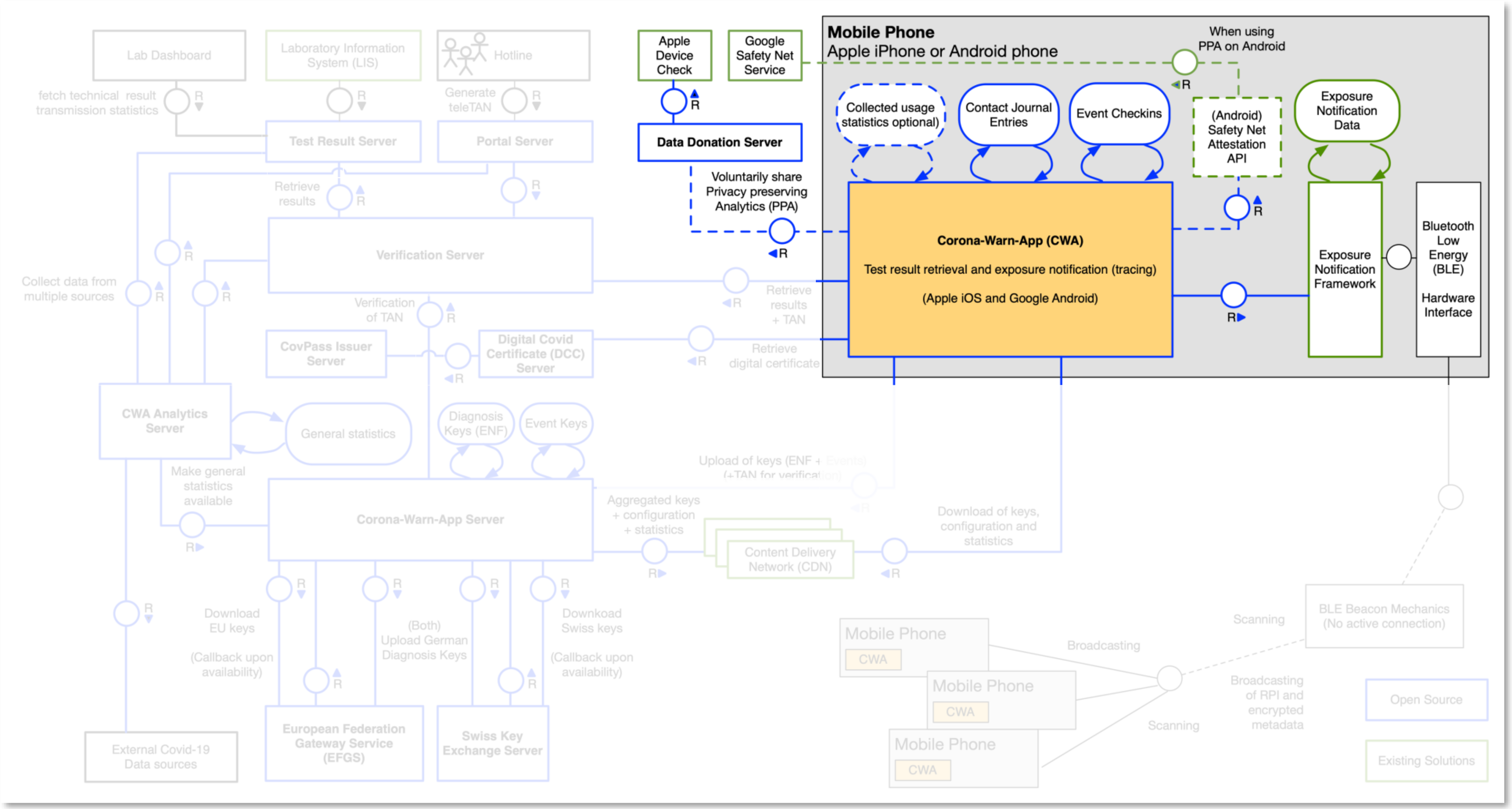
Android mobile app

- uses Google SafetyNet to attest device and app integrity
- increases attack complexity

Data Donation Server

- verifies cryptographic signature of attestation before storing

Architecture of PPA and EDUS for iOS Devices



iOS mobile app

- generates new API Token once per month
- submits data with API Token

Data Donation Server

- uses Apple Device Check to allow new API Token once per month per device
- checks rate limits of API Token

Event-Driven User Survey (EDUS)

Carried out between March and May 2021

Recruiting users who received a high-risk notification, aka “red warning”

26,094 participants completed the basic survey

15,561 completed the follow-up survey

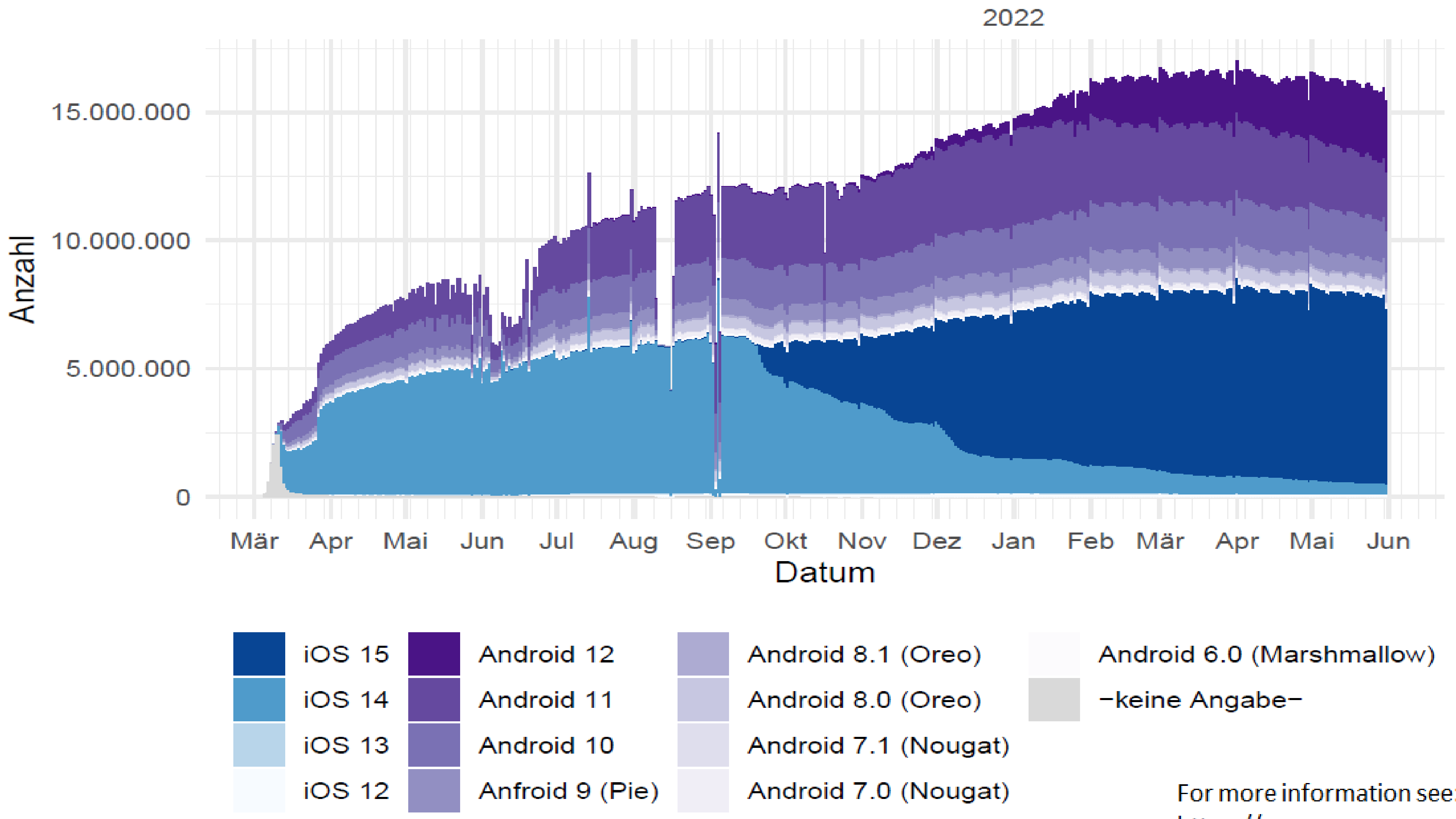
For more information see:

- https://www.coronawarn.app/en/science/2021-07-08-science-blog-2
- https://www.coronawarn.app/en/science/2021-08-02-science-blog-3

Selected findings:

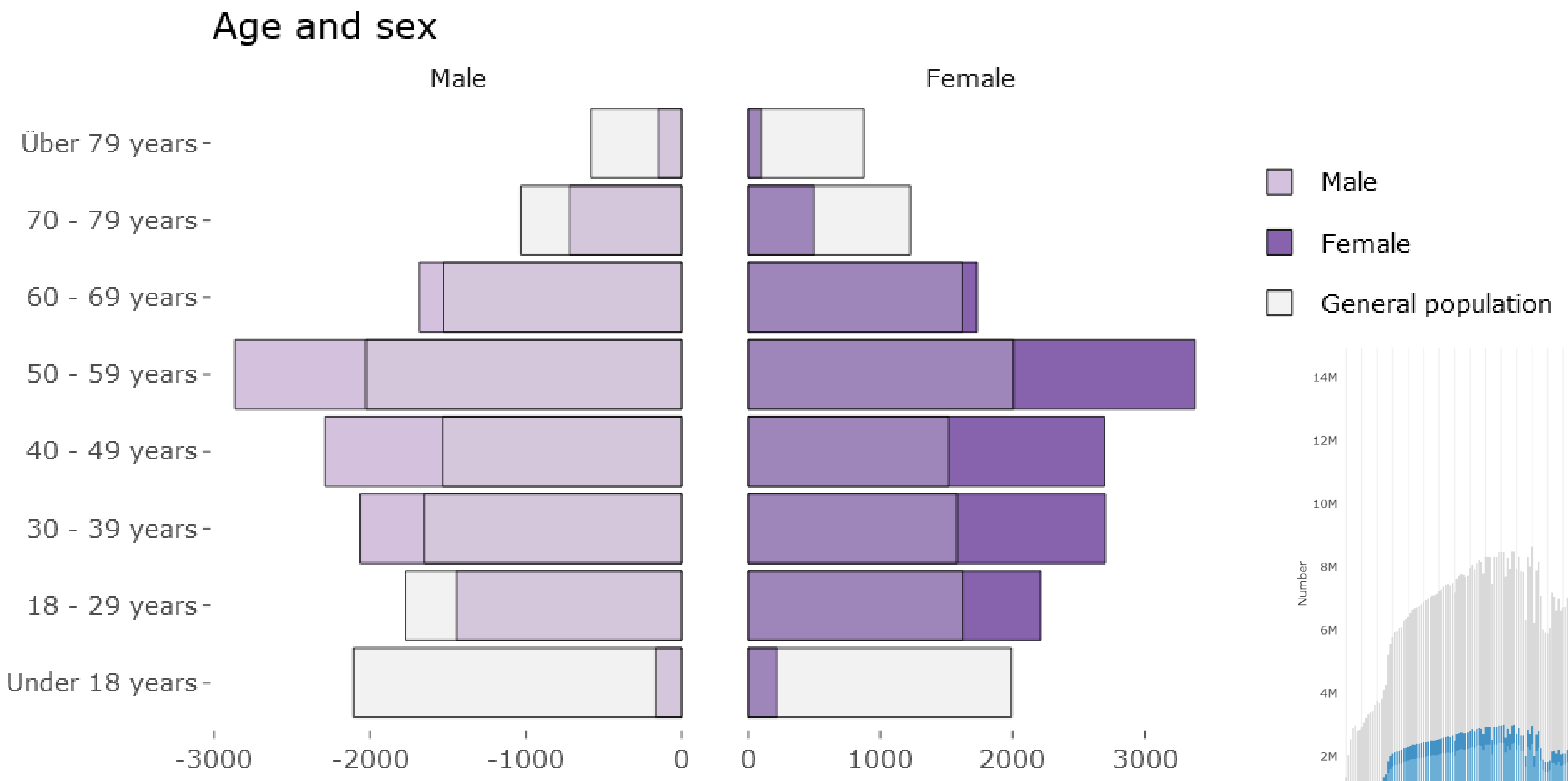
- 72.5% of the respondents were surprised to receive a "red warning".
- The majority of respondents adapted their behaviour to help prevent the virus from spreading.
- 68% stated that they intended to take a test immediately after having received a "red warning".
- 87% of the participants in the follow-up survey were tested as a direct result of receiving a "red warning".
- Respondents generally received their test results via the app within 24 hours.

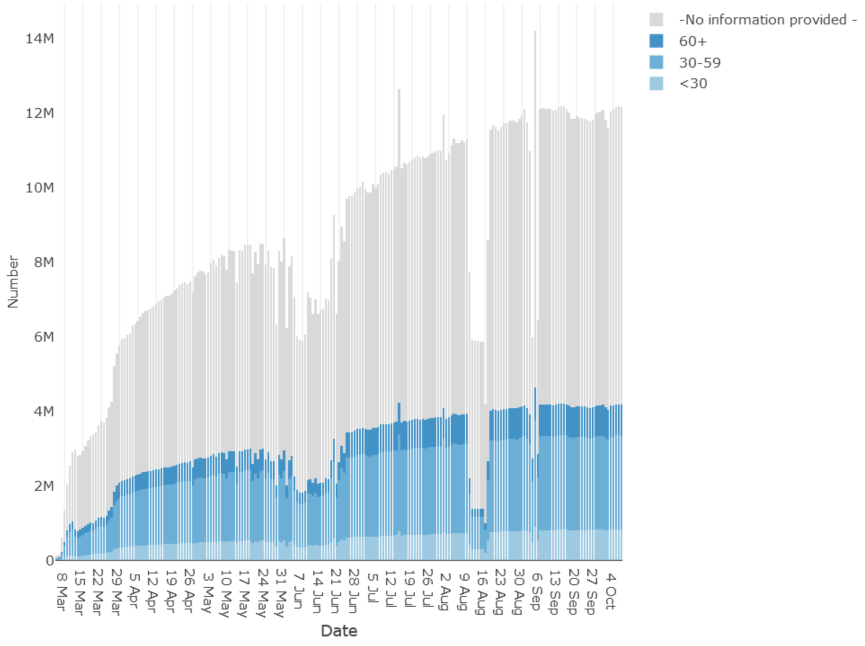
Privacy-Preserving Analytics: Devices by OS version (2021)



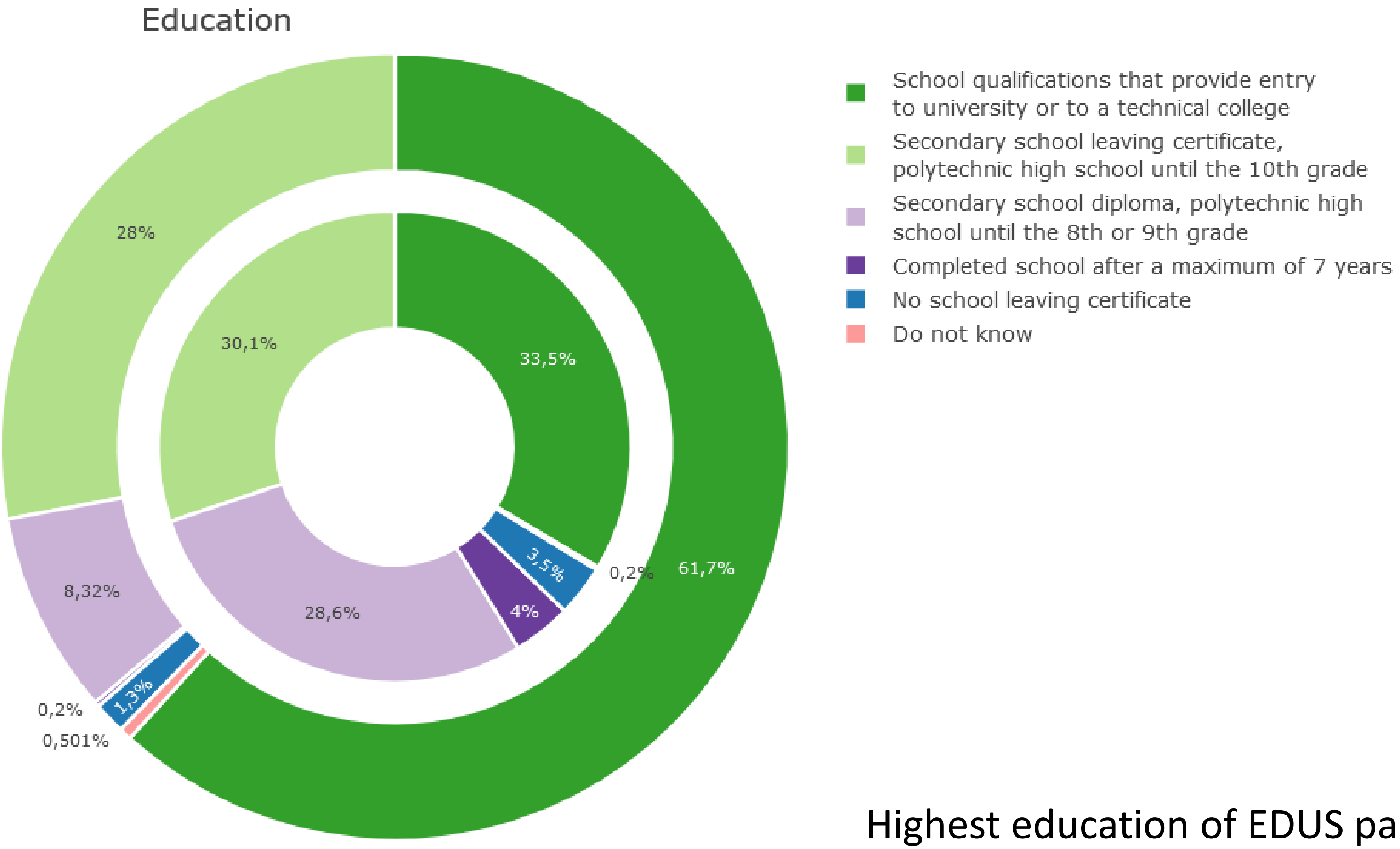
For more information see:
https://www.coronawarn.app/en/science/2021-10-15-science-blog-4

EDUS/PPA 2: Age groups and sex



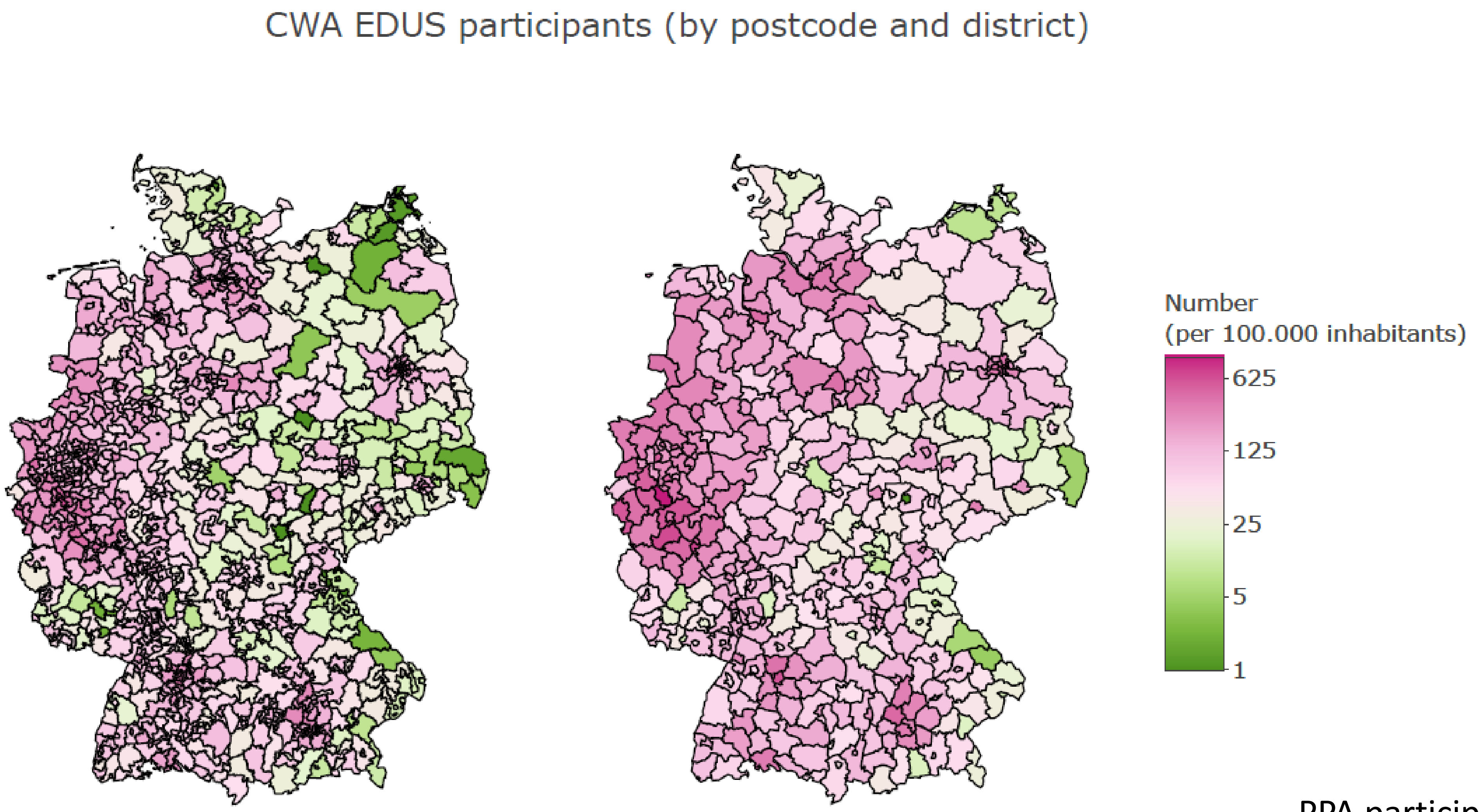


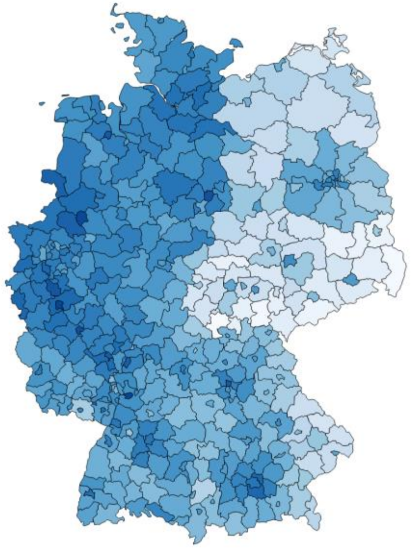
EDUS 3: Education



Highest education of EDUS participants (outer circle) compared to general population (inner circle)

EDUS/PPA 4: Spatial distribution





PPA participation rate on 31 Aug 2021

Outline

Part 1 – Introduction to Mobile Contact Tracing Apps (MCTA)

- Introduction to Digital Contact Tracing (DCT)
- DCT technologies and systems

Part 2 – Deploying country-wide MCTA: From theory to practice

- Google/Apple Exposure Notification (GAEN) framework
- Real-life implementation: The German Corona-Warn-App system

Part 3 – Performance evaluation and what is next

- Uptake and effectiveness of MCTA
- Cybersecurity and data privacy aspects
- Recent trends and future directions

Uptake of GAEN-based apps

UK's NHS COVID-19 app

- By end of Oct. 2020, the NHS COVID-19 app was downloaded by more than 19M users, i.e., more than **40%** of adults with access to a compatible smartphone
- In Autumn-Winter 2020 it was used regularly by approximately 16.5M users, i.e., **28%** of the total population
- At the end of 2020, it was the 2nd most-downloaded free app in the UK in Apple App store (behind Zoom and above TikTok)

By end of May 2022, **71** territories have deployed GAEN-based MCTA[1]

- 26 states in the USA (**2** recently discontinued)
- 25 EU countries (**7** discontinued/inactive by May 2022 including AT, CY, CZ, DK, PL, EE, and NL)[2]
  - France and Hungary operate non-GAEN centralized MCTA
  - **~23%** of EU citizens (~73M) have downloaded their GAEN-based national MCTA (max: **56%**)
- 20 other territories around the world (e.g., Canada, Brazil, Japan)

[1]Source: https://developers.google.com/android/exposure-notifications/apps
[2]eHealth Network statistics

Effectiveness of MCTA

Misconception from early studies that high adoption rates are needed (e.g., **56%** of the total population) to be effective[1]

Modeling in Washington state [USA, September 2020][2]

- Modeling by Google & Oxford University
- With 15% of the population participating, apps could reduce infections and deaths by approximately **8%** and **6%** (combined with traditional contact tracing and social distancing)

Study in Arizona State University [USA, autumn 2020][3]

- 46% of infected persons interviewed had the app and 55% of these app users shared their positive test result
- Apps could reduce the rate of infection *R* by **~12%** and would be a significant contribution to transmission control

[1]R. Hinch et al., Effective configurations of a digital contact tracing app: a report to NHSX, Aug. 2020. https://github.com/BDI-pathogens/covid-19_instant_tracing
[2]M. Abueg et al., Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state, MedRxiv, Sep. 2020.
[3]J. Masel et al., Quantifying meaningful adoption of a SARS-COV-2 exposure notification app on the campus of the university of arizona, medRxiv, Oct. 2021.

Effectiveness of MCTA

Smittestopp (non-GAEN version) [Norway, spring 2020][1]

- The tracing efficacy (i.e., the probability that a physical proximity event between two phones is detected by the app) was measured at **80%**
- At least **11%** of the discovered close contacts could not have been identified by manual contact tracing
- Significant impact even for moderate uptake numbers (e.g., 40% for R=1.5)

Radar Covid [Spain, summer 2020][2]

- 4-week population-based controlled experiment in La Gomera (Canary Islands)
- 7 KPIs: 5 for user behaviour (*adoption*, *adherence*, *compliance*, *turnaround time*, *follow-up*) and 2 for effectiveness (*overall detection*, *hidden detection*)
- At least 33% of the population adopted the technology, 349 simulated infections
- **6.3** close-contacts detected per primary simulated infection, a significant percentage being contacts with strangers (~3 manually traced contacts in Spain)

[1] A. Elmokashfi et al., Nationwide rollout reveals efficacy of epidemic control through digital contact tracing, Nature Communications, Oct. 2021.
[2] P. Rodríguez et al., A population-based controlled experiment assessing the epidemiological impact of digital contact tracing, Nature Communications, Jan. 2021.

Effectiveness of MCTA

NHS COVID-19 [England and Wales, autumn-winter 2020][1]

- 1.7M notifications sent, i.e., ~4 per positive case consenting to contact tracing
- **6%** of individuals notified by the app subsequently showed symptoms and tested positive (i.e., secondary attack rate) that is similar to manual contact tracing
- For every 1% increase in app users, the number of infections can be reduced by **0.8%** (modelling) or **2.3%** (statistical analysis)
- Public Health message is clear: ‘Use the app, it works’.

SwissCovid [Switzerland, June 2021][2]

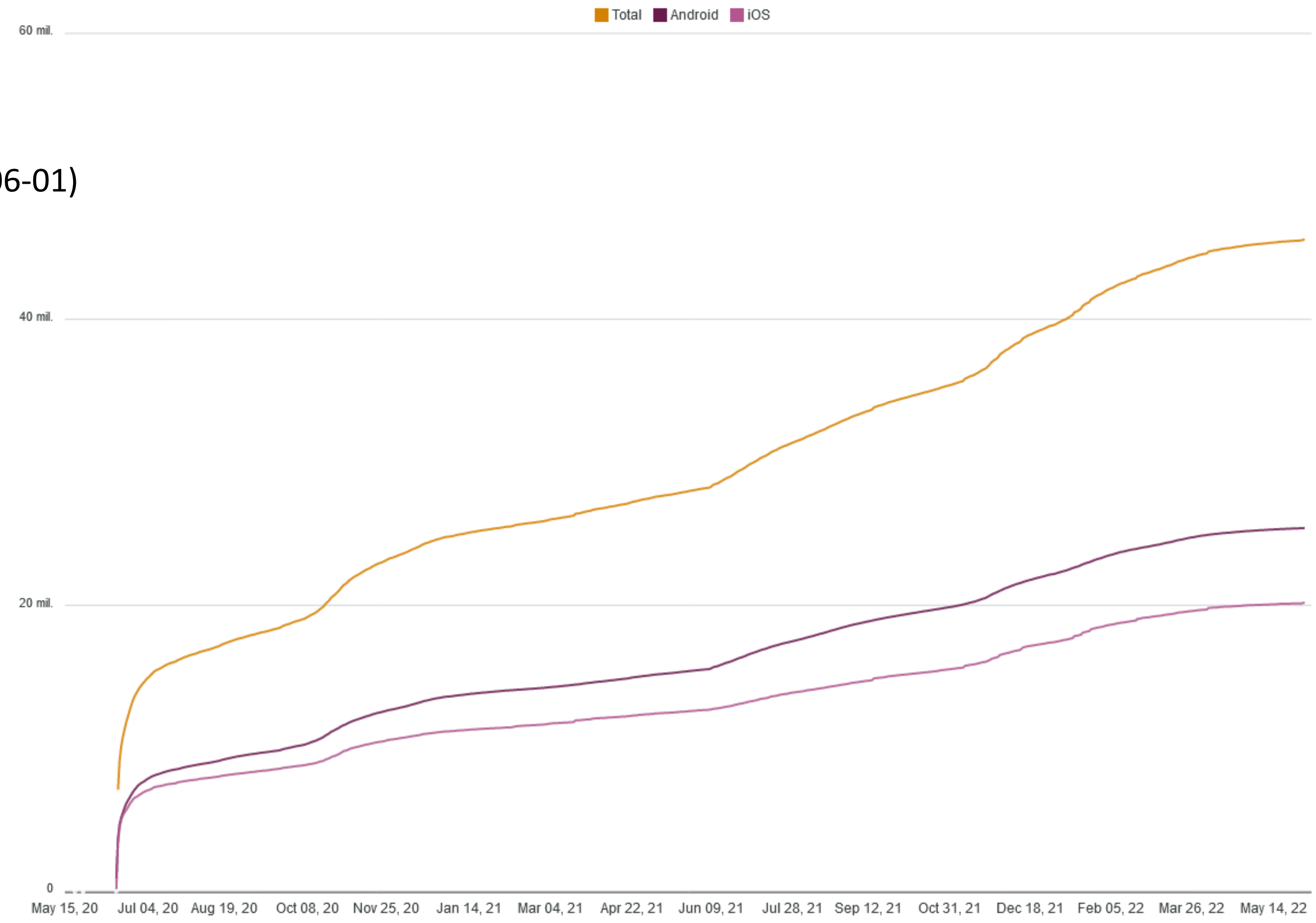
- Contributed to preventive actions in **76%** of exposure notification recipients and were associated with a faster quarantine time in some user groups
- Estimated to have contributed to the notification and identification of 500 to 1000 positive app users per month (lower than UK and Germany)

What about the uptake and effectiveness of CWA?

[1]C. Wymant et al., The epidemiological impact of the NHS COVID-19 App, Nature, May 2021
[2]P. Daniore et al., The SwissCovid Digital Proximity Tracing App after one year: Were expectations fulfilled?, Swiss Medical Weekly, Sep. 2021.

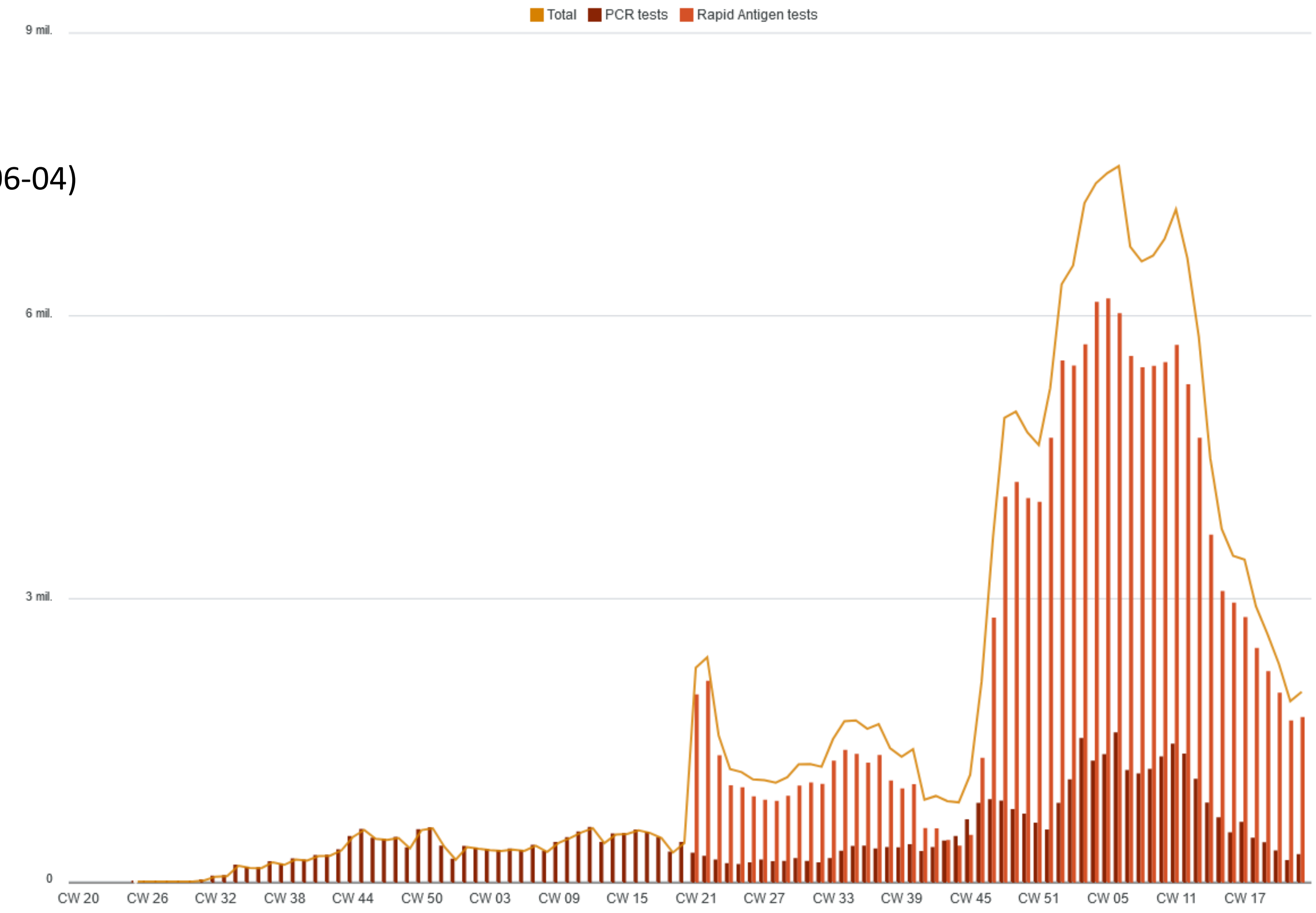
CWA Public dashboard: Cumulative downloads, by OS

45,591,924
Total (count until 2022-06-01)



CWA Public dashboard: Test results provided, by type, by week

194,616,952
Total (count until 2022-06-04)

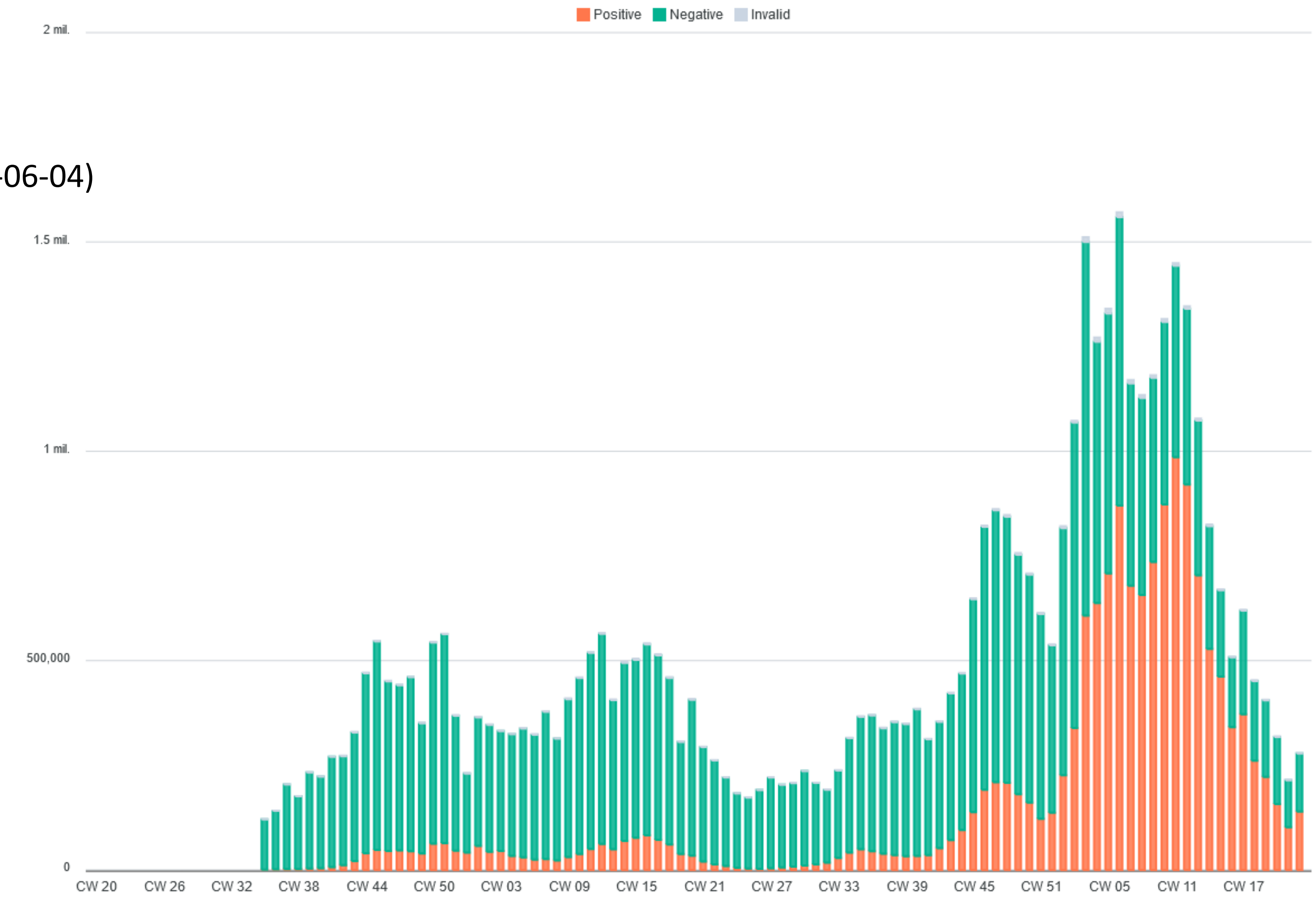


2020 2021 -> 2022 ->

CWA Public dashboard: PCR test results provided (pos, neg, ind/inv), by week

48,286,814

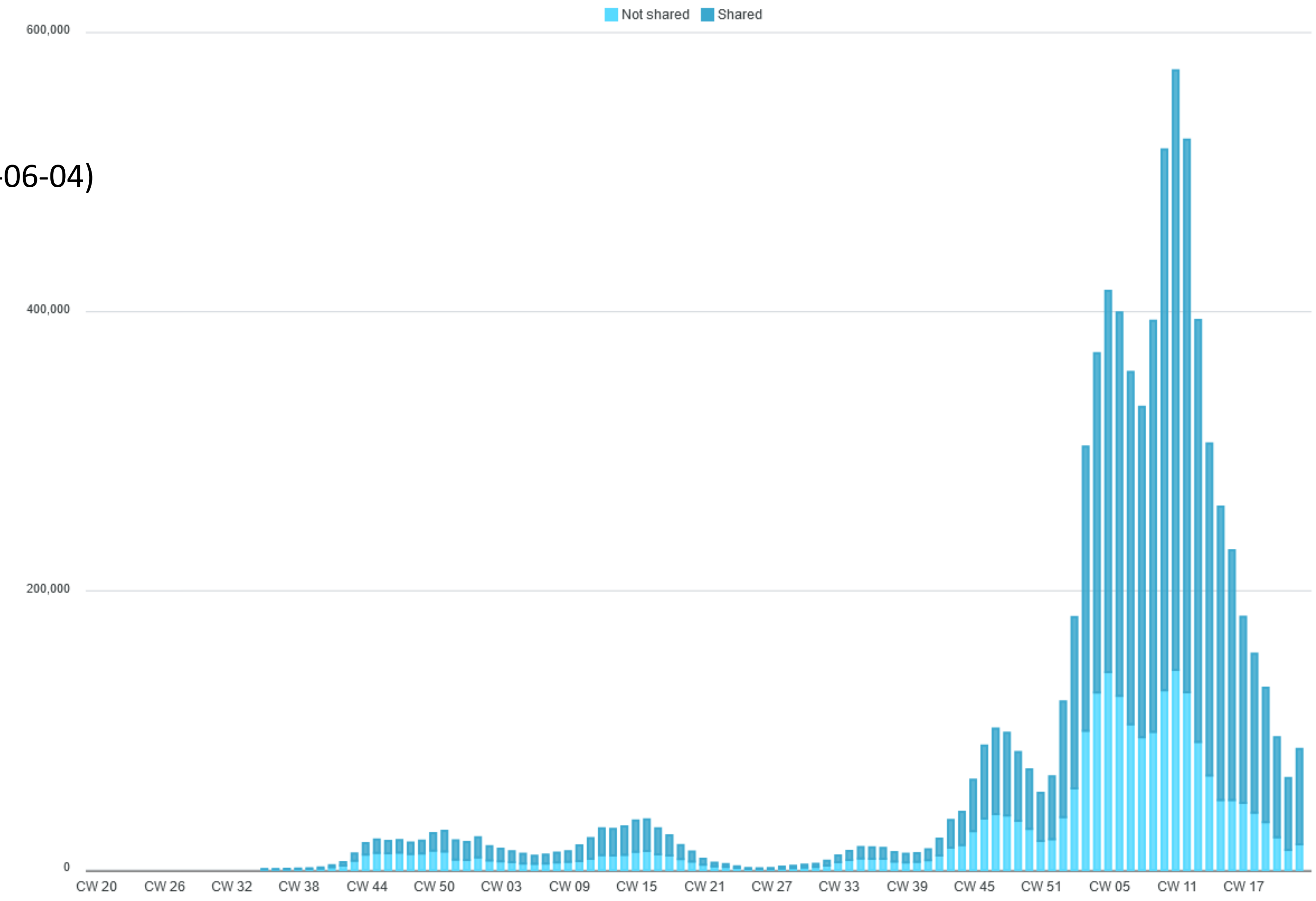
Total (count until 2022-06-04)



2020 2021 -> 2022 ->

CWA Public dashboard: Positive test results in-app verified for sharing (key upload), by week

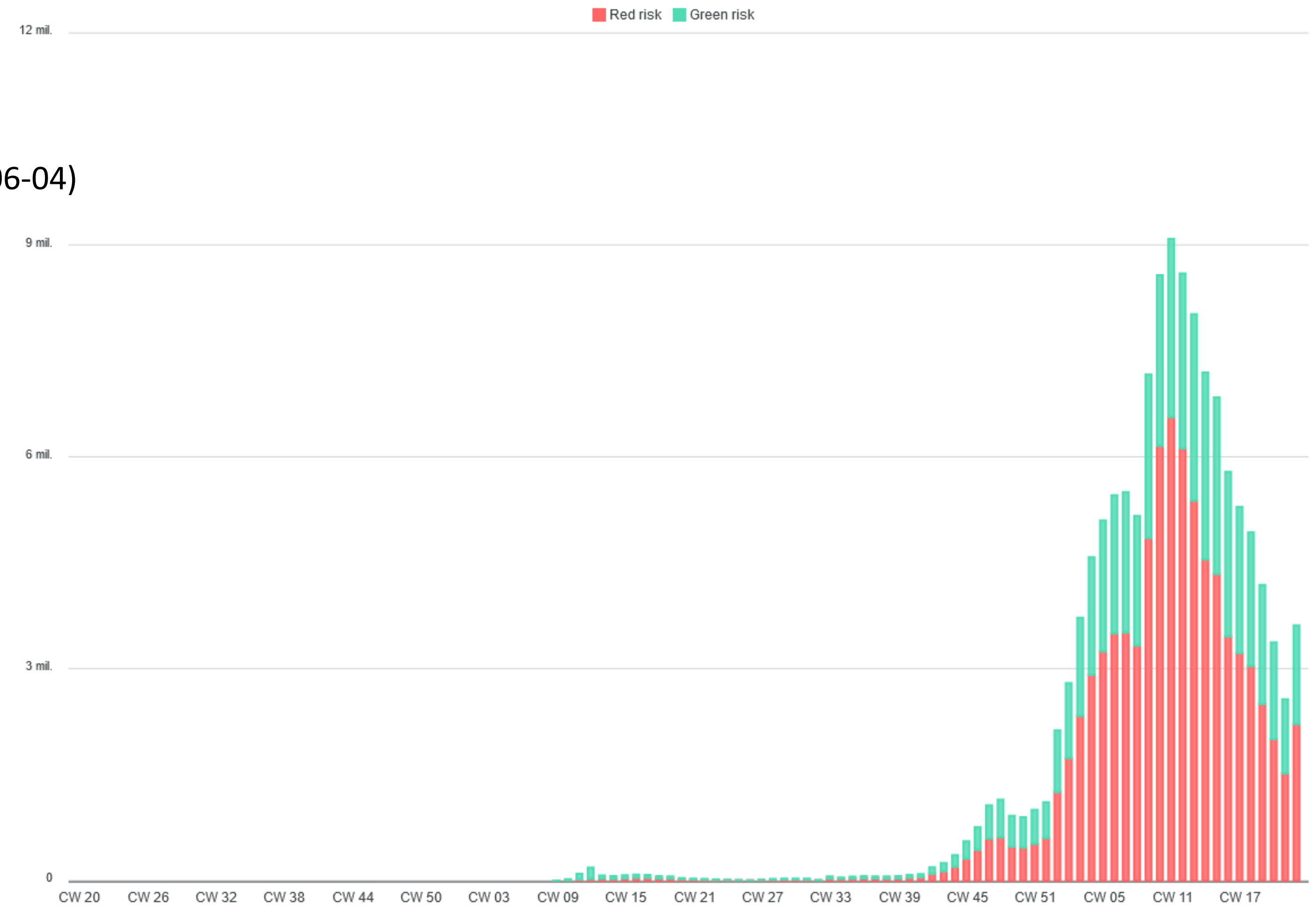
7,950,455
Total (count until 2022-06-04)



2020 2021 -> 2022 ->

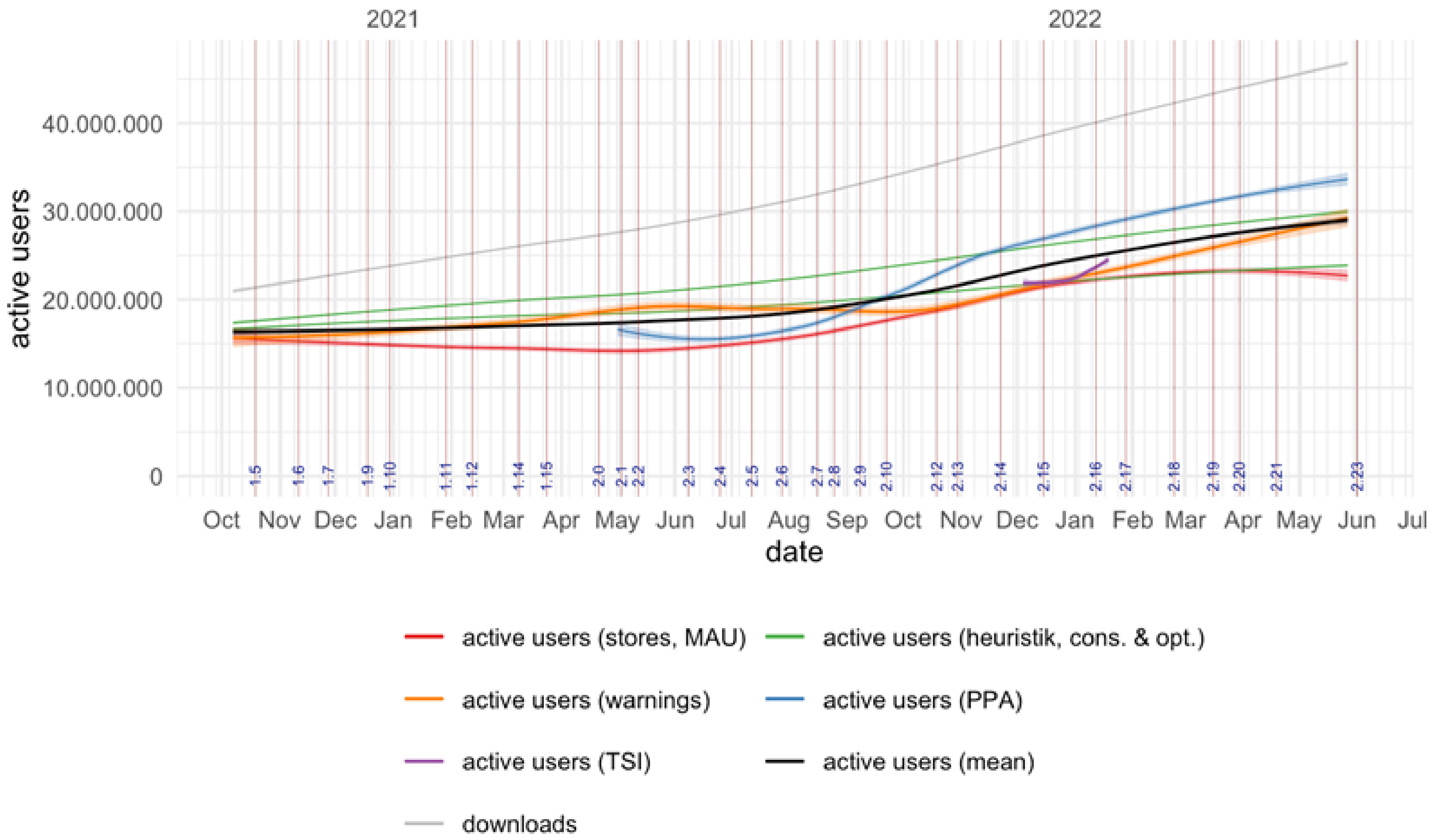
CWA Public dashboard: Notifications received by data donors, by risk level, by week

129,514,698
Total (count until 2022-06-04)



2020 2021 -> 2022 ->

Active users



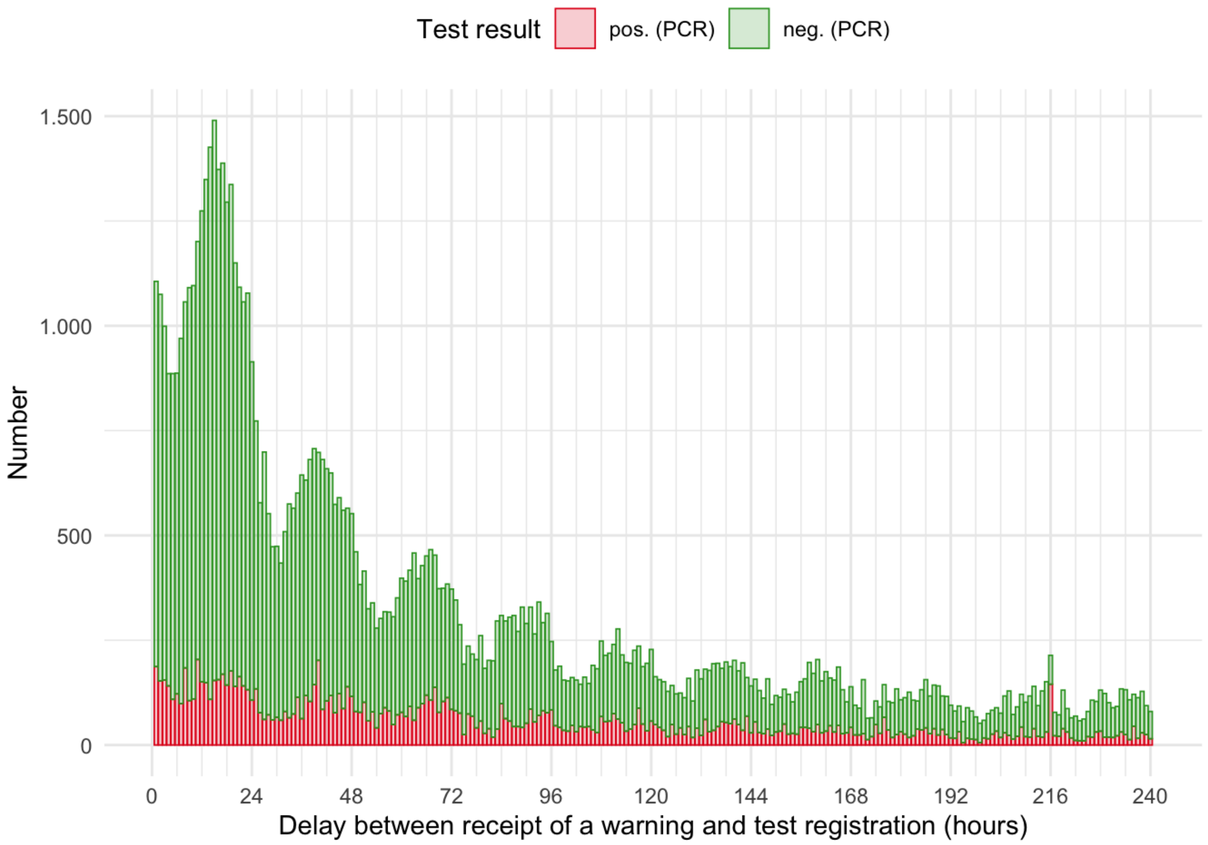
Estimates derived from different sources and methods

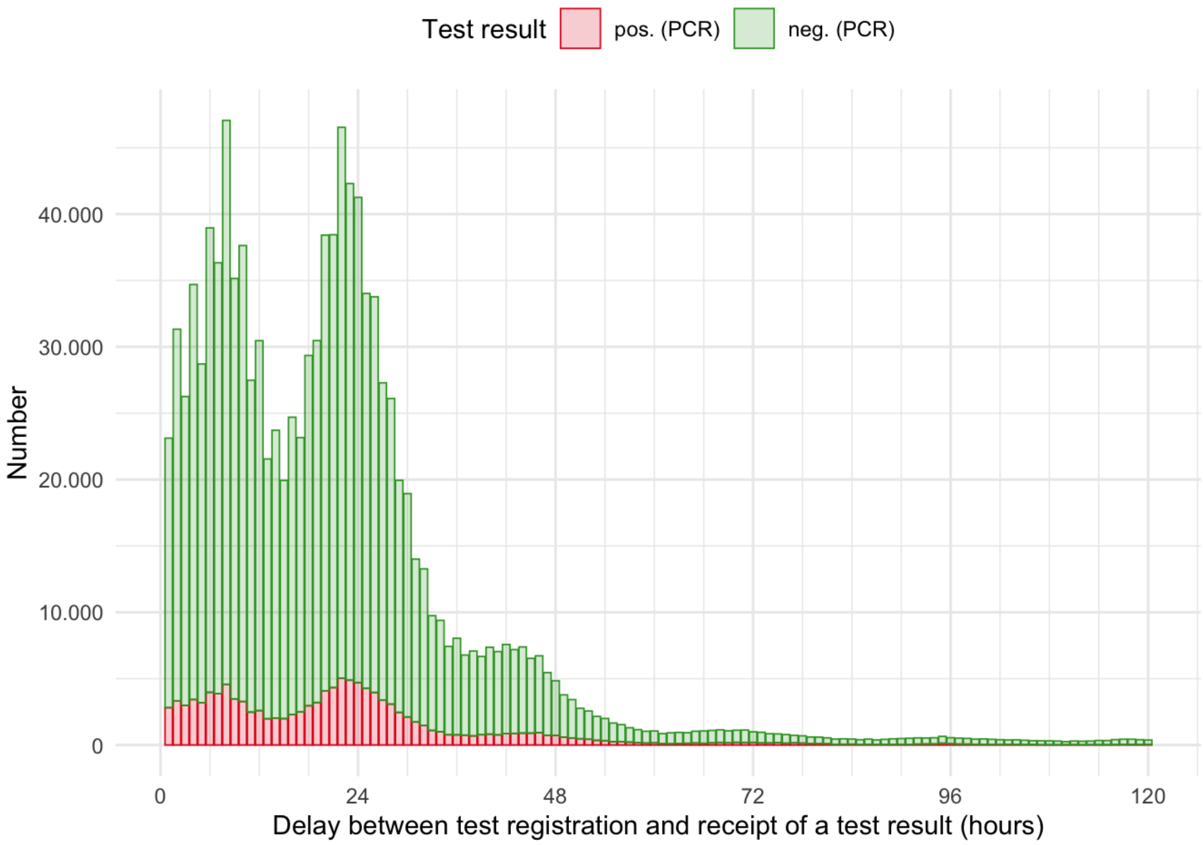
- [red] from store statistics (MAU = Monthly Active Users)
- [green] from downloads (considering attrition)
- [orange] from key uploads compared to notified infections
- [blue] from data donations
- [violet] from backend data traffic
- [black] **mean**

NB: Active users are fewer than active devices

For more information see:
https://www.coronawarn.app/en/science/2022-03-03-science-blog-5

Testing delays

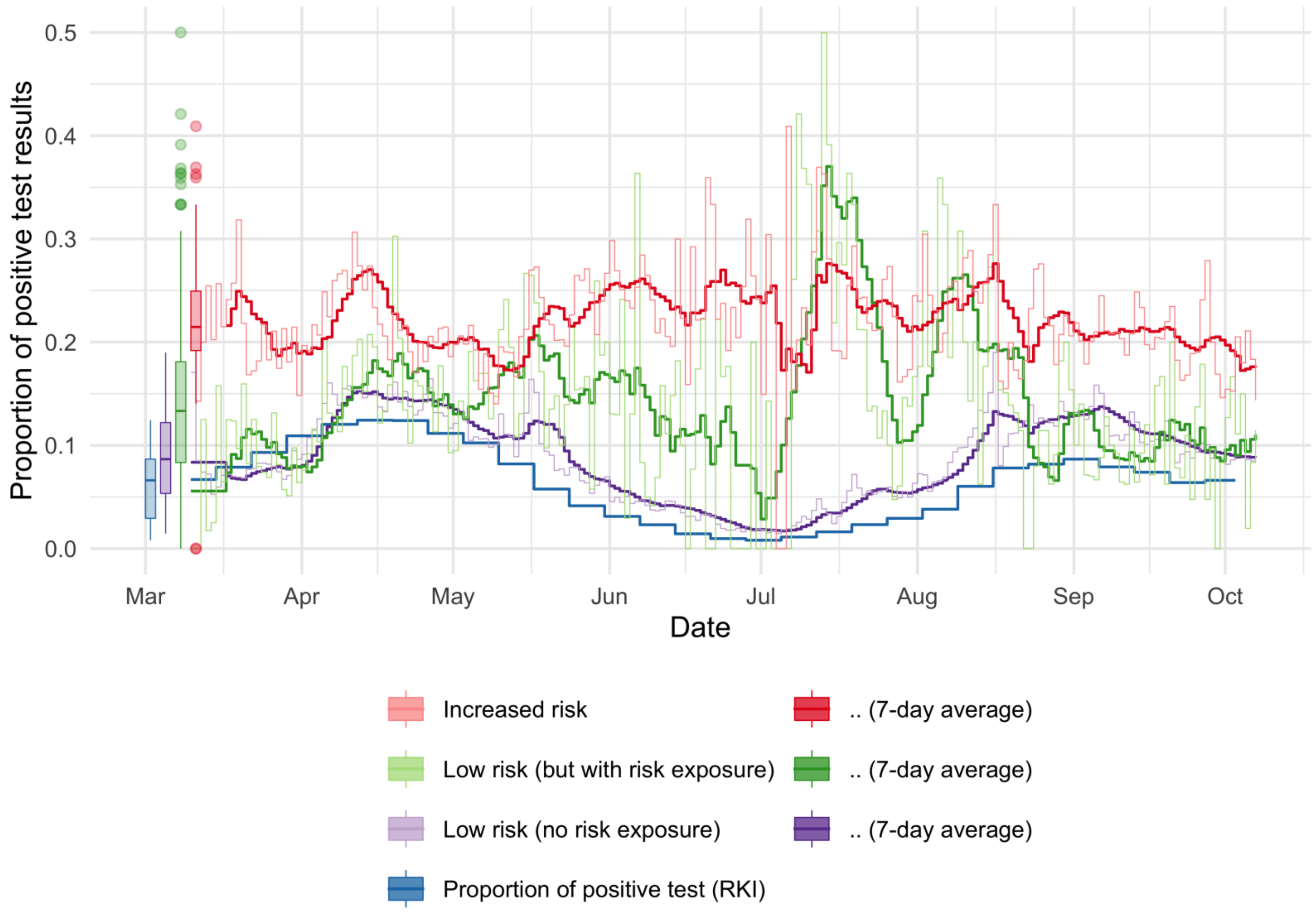




Referred to as "Follow-up" KPI in the study of the Spanish Radar Covid MCTA[1]
The ECDC/WHO indicator framework does not include it, but the eHN suggest to add it as "D5: Adherence to testing guidelines"

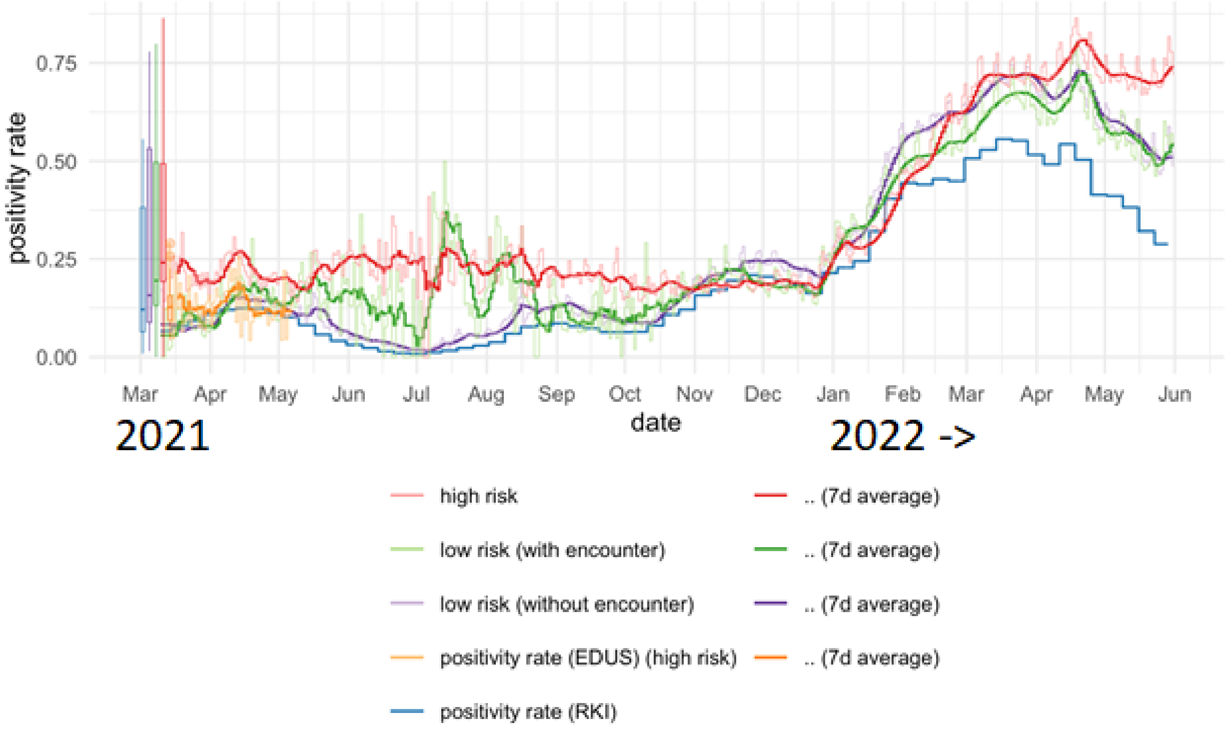
[1]P. Rodríguez et al., A population-based controlled experiment assessing the epidemiological impact of digital contact tracing, Nature Communications, Jan. 2021.

Proportion of positive tests by risk level 1/2

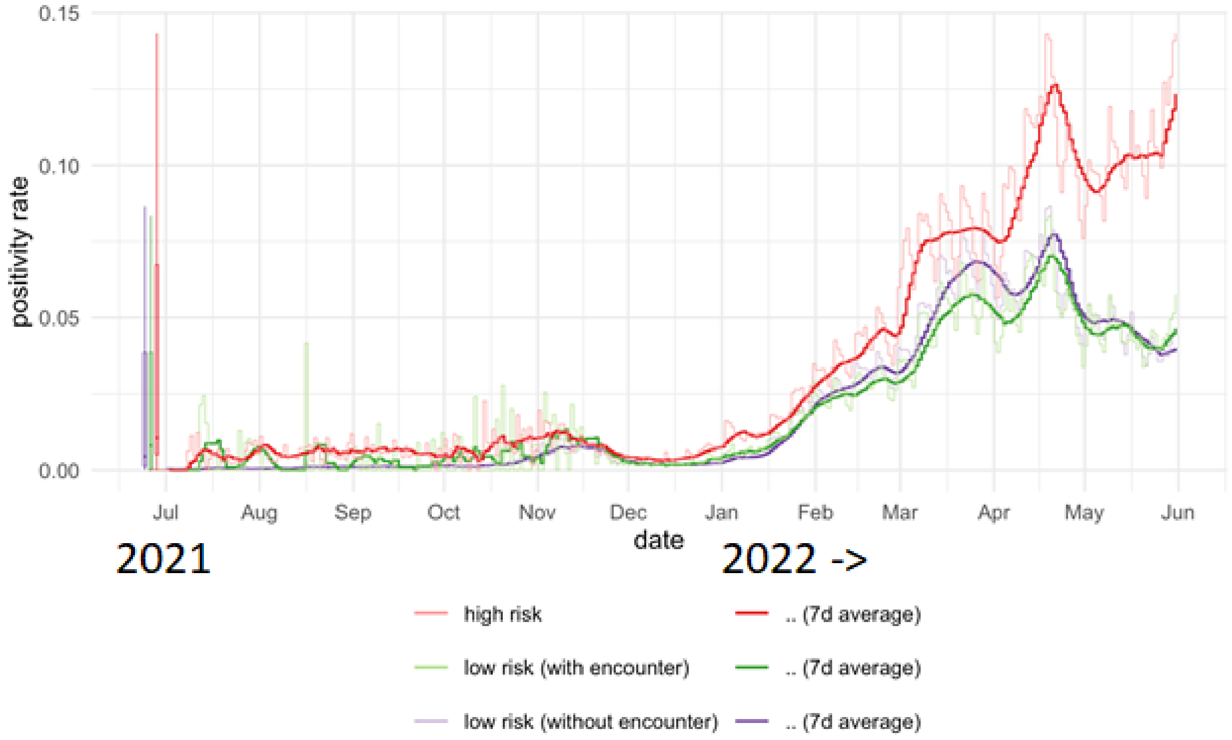


Proportion of positive tests by risk level 2/2

PCR tests



Rapid antigen tests



Lessons learned

- Define key performance and effectivity indicators early on
- Enable ongoing collection of relevant data for M&E
  - infrastructure and procedures
- Ideally standardize between systems for comparability
  - Indicator framework to evaluate the public health effectiveness of digital proximity tracing solutions by WHO/ECDC[1]
  - Monitoring framework for measuring the use and performance of digital contact tracing solutions in the EU by the eHealth Network (under preparation)
    - Extends the WHO/ECDC framework with additional indicators

[1]Indicator framework for the evaluation of the public health effectiveness of digital proximity tracing solutions. Geneva: World Health Organization and European Centre for Disease Prevention and Control; 2021. Licence: CC BY-NC-SA 3.0 IGO.

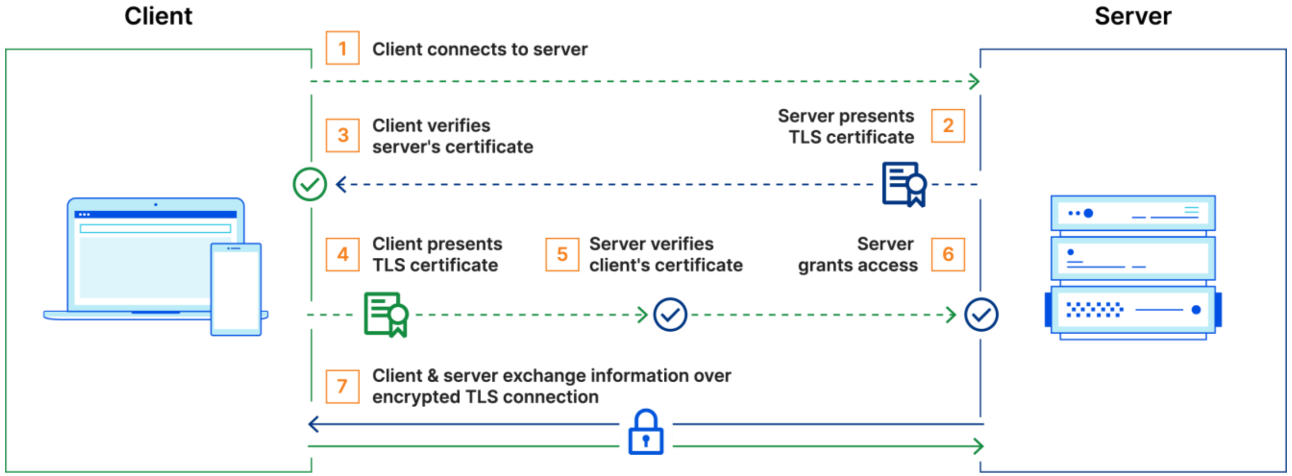
Digital Contact Tracing Cybersecurity

Cybersecurity attacks on digital contact tracing apps can have a big impact on the population

- Sensitive medical data leakage
- False data injection
  - Economic impact
  - Disruption of normal operation
  - Force governments to take wrong decisions
- Imitate someone else

Image source: Pittsburgh Post-Gazette, Contact tracing by app: life-saving or invasion of privacy? https://www.post-gazette.com/news/covid-19/2020/05/10/Contact-tracing-by-app-life-saving-or-invasion-of-privacy/stories/202005100052 Accessed 2022-06-06.

Mutual Transport Layer Security (mTLS)



- mTLS Prevents the following attacks:

Attack	Impact
Man in the Middle Attack	Steal all the data transmitted between the client and the server, inject false data, prevent data from reaching their destination
Imitation Attack	Imitate a sender or a recipient and steal data or inject false data
Leaked Credentials	Use leaked credentials to gain access as a client/server and steal data or inject false data
Phishing Attack	Gains access to credentials through a phishing attack and steal data or inject false data
Brute Force Attack	Gains access to the system by brute forcing the credentials and steal data or inject false data
Malicious API Requests	Imitate a trusted user and inject the system with false data or steal data using API requests

Image source: Cloudflare https://www.cloudflare.com/en-gb/learning/access-management/what-is-mutual-tls/ Accessed 2022-05-20.

Centralized Vs Decentralized Solutions

Centralized:

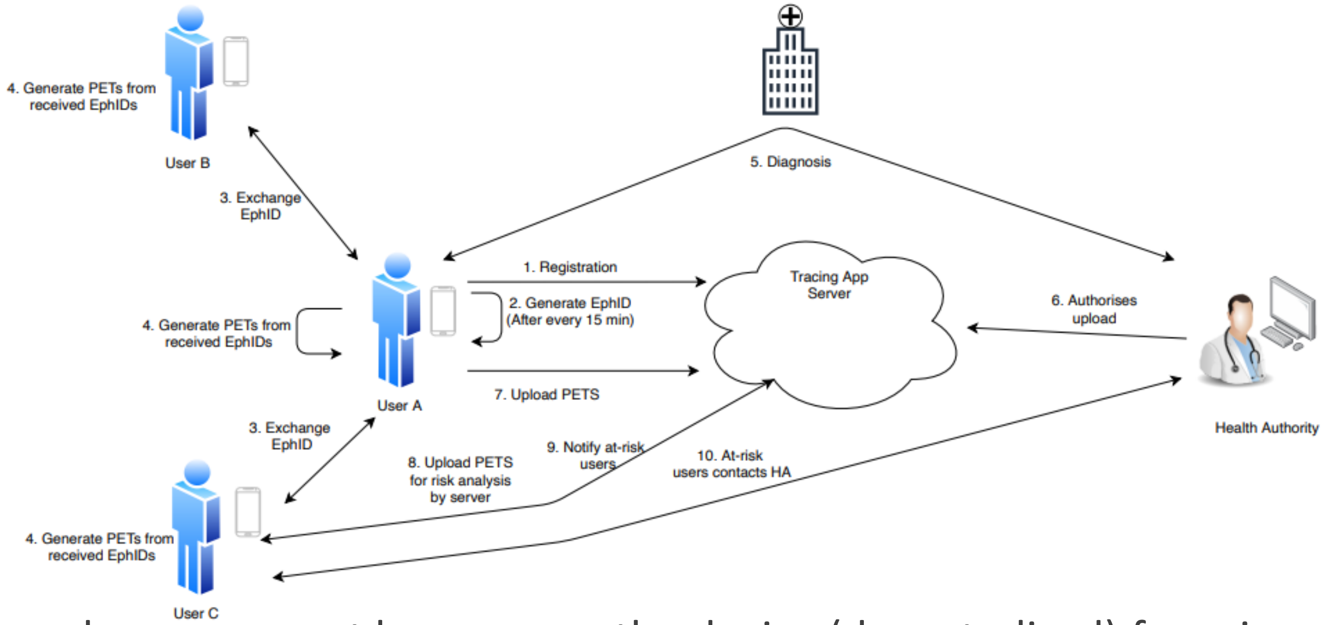
- All potentially identifying information is stored in the server, while individual apps hold little information about the user.
- If the server was successfully compromised, or if the body overseeing the server uses the information maliciously, individual phones and their owners can be identified and associated with specific temporary IDs.
- Privacy risks such as identifying infected individuals and determining a user's social circle may be occur.
- A malicious actor trying to access information stored in an individual app wouldn't be able to learn anything about the user of the app.

Decentralized:

- The apps store a cache of temporary IDs that have been sent out, while the server holds only the temporary IDs of positively infected users.
- By the design of the system, infected users give up a level of privacy, as the server publishes the temporary IDs of infected users for all apps to check.
- The server won't have any information on uninfected users that can be used maliciously.
- Because the temporary IDs cannot be immediately removed from a phone, a hacker that breaks into an individual phone would be able to learn the temporary IDs associated with the user.

Source: Serge Vaudenay "Centralized or Decentralized? The Contact Tracing Dilemma" EPFL, Lausanne, Switzerland

Hybrid Architecture



- TempID generation and management happens on the device (decentralized) for privacy and anonymization
- Risk analysis & notification is performed on the server
  - In the risk analysis the server is aware of the number of at-risk users, thus it has all the statistical information needed to run data analytics to identify exposure clusters
  - Risk analysis and notifications are considered a sensitive process that should be handled by the authorities, keeping the existing infrastructure resources and state of the pandemic in mind
  - The uploaded encounter information from infected users is not made available to the other users but retained only at the server. This is to avoid user de-anonymisation attacks which can be possible in the decentralised architecture

Image source: N. Ahmed et al., "A Survey of COVID-19 Contact Tracing Apps," in IEEE Access, vol. 8, pp. 134577-134601, 2020.

Risk Analysis of Known Attacks per Architecture

Attack / Architecture	Centralized	Decentralized	Hybrid
Replay & Relay	5	4	5
Wireless Tracking	5	4	5
Location Confirmation	4	1	1
Enumeration	2	2	1
DoS	5	4	5
Linkage	4	5	2
Carryover	3	2	2
Social Graph	4	1	1

Risk level of an attack for each architecture

Risk Impact Level	1	2	3	4	5
Percentage of App Affected	0-20%	21-40%	41-60%	61-80%	81-100%

Risk impact level key

Relay/Replay attack

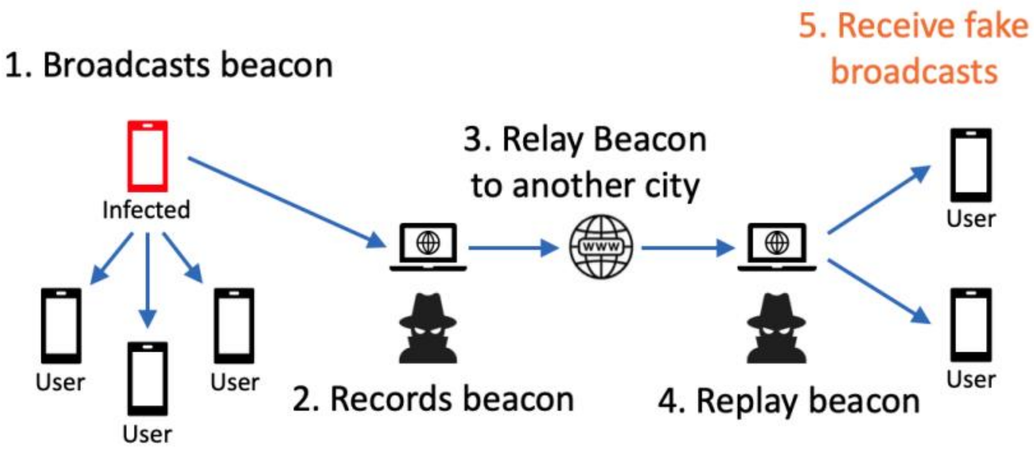


Image source of Risk Analysis: Created based on data provided by N. Ahmed et al., "A Survey of COVID-19 Contact Tracing Apps," in IEEE Access, vol. 8, pp. 134577-134601, 2020.
Image source of Replay/Relay Attack: R. Sun, et al., An Empirical Assessment of Global COVID-19 Contact Tracing Applications, Proceedings of the 43rd International Conference on Software Engineering, 2021, 1085–1097.

Known Vulnerabilities

- The encrypted metadata block with a TX value lacks a checksum, allowing bit flipping to amplify a contamination attack. This can cause metadata deanonymization and risk-score inflation. Google/Apple Response: “We do not believe that TX power authentication would be a useful defense against relay attacks” (CVE-2020-24722)
- On Android attackers are allowed to obtain sensitive information, such as a user's location history, in-person social graph, and (sometimes) COVID-19 infection status, because Rolling Proximity Identifiers and MAC addresses are written to the Android system log, and many Android devices have applications (preinstalled by the hardware manufacturer or network operator) that read system log data and send it to third parties. Vendor fixed the Vulnerability (CVE-2021-31815, GAEN potential vulnerability report by AppCensus)

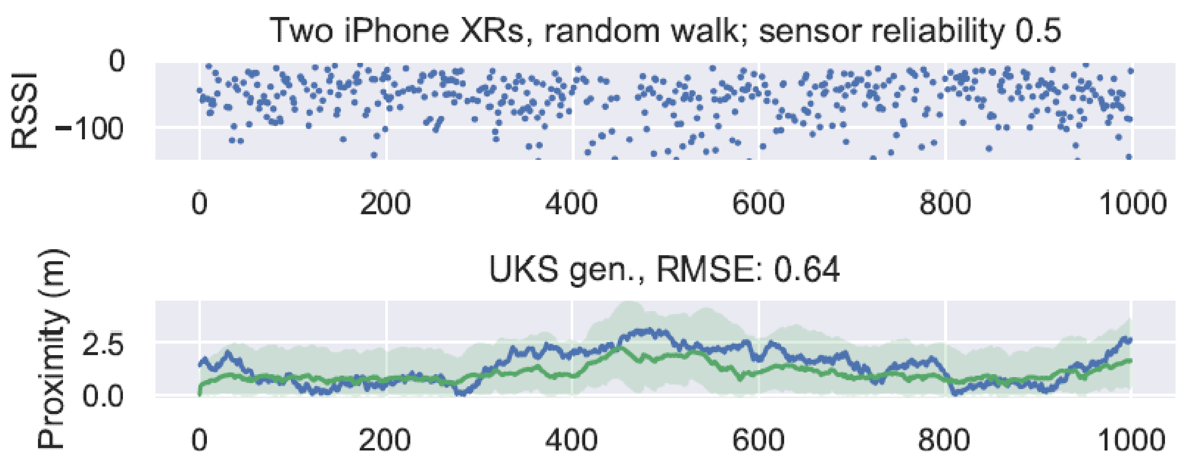
```
W ExposureNotification: getCurrentRollingProximityId: generated a new
RollingProximityId=768D2E1DC786F9FD6ACE4A17B37CDDE4 [CONTEXT service_id=236
]

W ExposureNotification: Scan device 46:DB:4A:02:27:97, type=1,
id=FDBF4CD00BD69C9BA8CC1BFEB208B291, raw_rssi=-88, calibrated_rssi=-92,
meta=4C8C70B1, previous_scan=1615224148 [CONTEXT service_id=236 ]
```

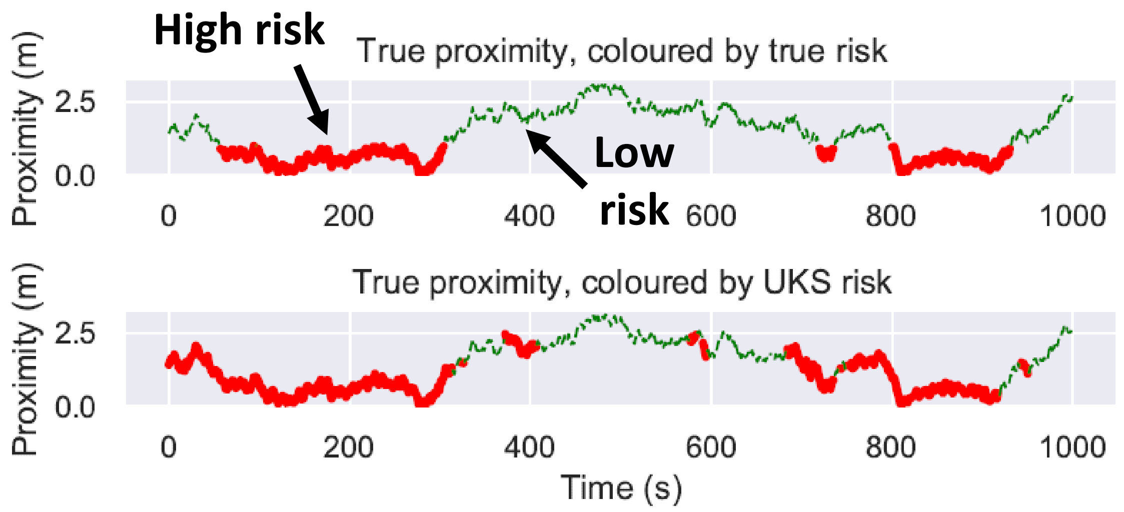
Image source: AppCensus Potential Data Breach of Contact-Tracing Data Report April 12, 2021

Improving existing MCTA
3.5G: Enhanced risk calculation

Enhancements in the NHS COVID-19 app (pre-GAEN)

- Probabilistic risk score model[1]
- Unscented Kalman Smoother with generative observation model for inferring proximity from BLE RSSI readings[2]
- Not fully feasible in the current GAEN implementation (e.g., timestamps of scans and median/min signal strength values are available)





[1]Briers, M. et al., Risk scoring calculation for the current NHSx contact tracing app. *arXiv preprint arXiv:2005.11057, 2020*.
[2]Lovett, T. et al., Inferring proximity from Bluetooth low energy RSSI with unscented Kalman smoothers. *arXiv preprint arXiv:2007.05057, 2020*.

Improving existing MCTA
3.5G: Presence tracing

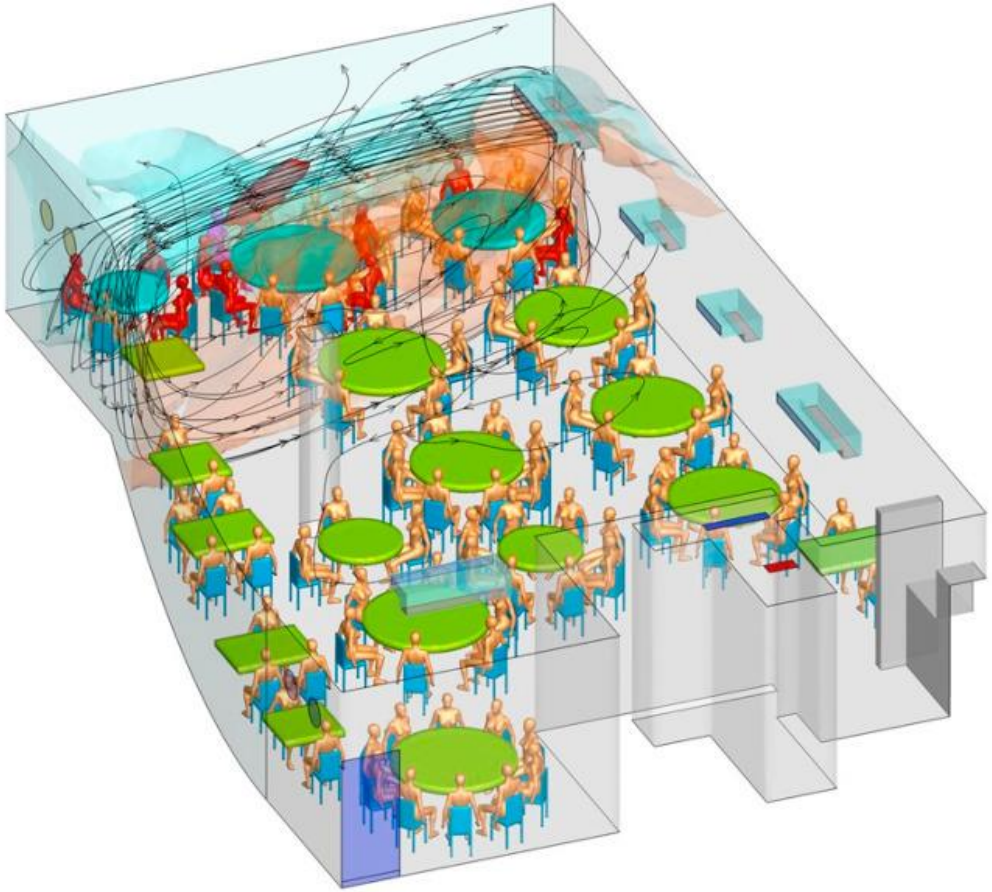
The process of identifying the source of infection of the case under investigation, to identify further cases and contacts (aka *bidirectional*, *retrospective*, or *backward* tracing)

A relatively small proportion of cases is responsible for a large proportion of transmission

- in indoor spaces where many people come together[1] (e.g., offices, theaters/cinemas, restaurants, bars/clubs, public transportation, etc.)
- in the so called cluster or super-spreading events[2] (e.g., concerts, sport games, wedding/birthday parties, etc.)
- “fleeting” contacts leading to transmission of the Delta variant[3]

How effective could it be?

- Adding backward contact tracing could make ‘forward’ standard contact tracing **2-3 times** more effective in the UK context[4]



[1]Y. Li, et al., Probable airborne transmission of sars-cov-2 in a poorly ventilated restaurant, Building and Environment, vol. 196, p. 107788, 2021.
[2]S. L. Miller, et al., Transmission of sars-cov-2 by inhalation of respiratory aerosol in the skagit valley chorale superspreading event,” Indoor Air, vol. 31, no. 2, pp. 314–323, 2021.
[3]Lu, D. COVID Delta variant is “in the air you breathe”: What you need to know about Sydney outbreak strain. The Guardian (2021), https://bit.ly/3xoaFZ0
[4]E. Akira et al., Implication of backward contact tracing in the presence of overdispersed transmission in COVID-19 outbreaks, Wellcome open research, Mar. 2021.

Improving existing MCTA
3.5G: Presence tracing

App users voluntary reporting their location or attendance to a venue/event
- Logbook of places visited in the past few days

Correlating location coordinates collected by GPS-based apps with public places or events

"Check-in" to a place using the smartphone camera to scan a location-specific QR code
- Current state-of-practice: CrowdNotifier[1] (CH-SwissCovid), CLEA[2] (FR-TousAntiCovid), server-based CrowdNotifier[3] (DE-CWA)

Devices exchanging Bluetooth signals similar to MCTA
- *Lighthouses*: proprietary Bluetooth-based protocol[4]
- Bluetooth-enabled IoT devices that propagate exposure notifications reaching all visitors through their MCTA[5]

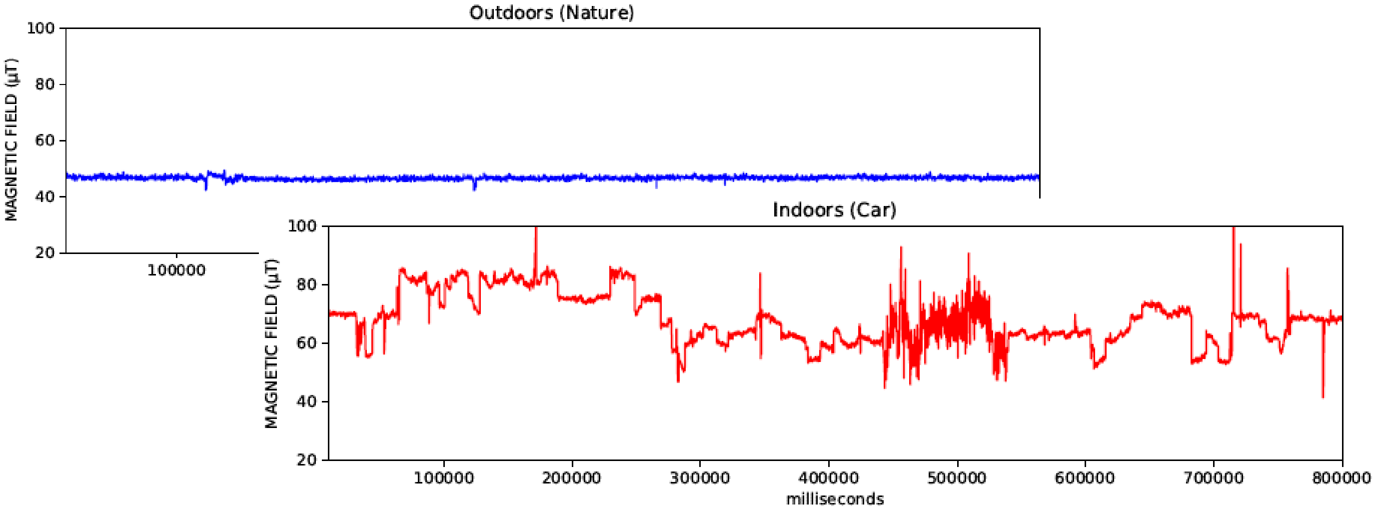
[1]W. Lueks, et al., CrowdNotifier: Decentralized privacy-preserving presence tracing, Proceedings on Privacy Enhancing Technologies, vol. 2021, no. 4, pp. 350–368, 2021.
[2]V. Roca, et al., The Cluster Exposure Verification (Clea) Protocol: Specifications of the Lightweight Version, 2021.
[3]CrowdNotifier - Decentralized Privacy-Preserving Presence Tracing, https://github.com/CrowdNotifier/documents#new-variants-of-crowdnotifier
[4]E. L. Reichert, et al., Lighthouses: A warning system for super-spreader events, in IEEE International Conference on Communications Workshops (ICC Workshops), 2021, pp. 1–6.
[5]C. Laoudias et al., Privacy-Preserving Presence Tracing for Pandemics Via Machine-to-Machine Exposure Notifications, IEEE ALIAS workshop, 2022.

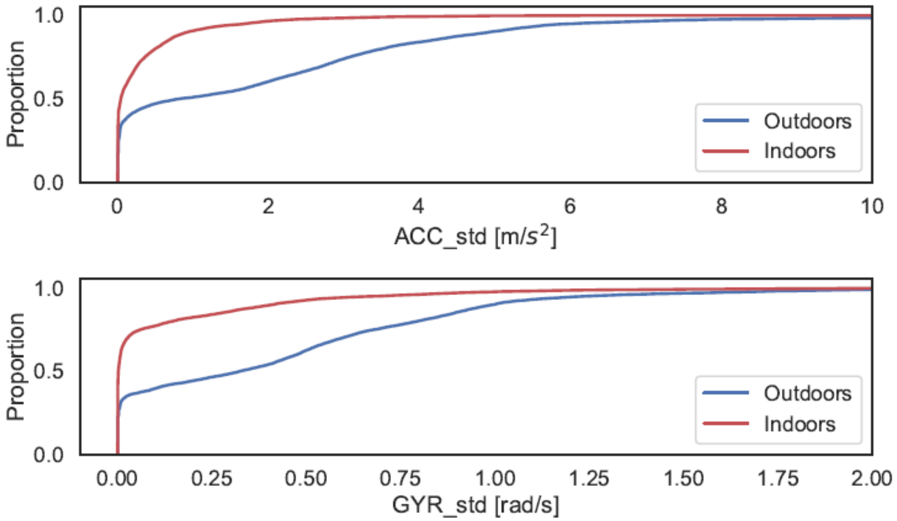
Improving existing MCTA
3.5G: Indoor/Outdoor classification

Indoor/outdoor classification → need to preserve privacy and be energy efficient
- Speaker and Microphone raise privacy concerns
- GPS and Wi-Fi may significantly reduce battery life

Sensors: GPS, RF, light, magnetometer, IMU → Typical accuracies ~85%

Accelerometer + gyroscope + light sensor: Accuracy 85% (outdoors) and 75% (indoors)[1]
- Should reach 90%-95% accuracy to make it into future MCTA
- The possibility of CO_2 sensor integration (Apple patent) could increase classification accuracy





[1]Briers et al., Indoor/Outdoor Detection for Covid-19 Contact Tracing Apps, 2020.

4G – Promising technologies for next-gen MCTA:
General

General

- Smartphones and other mobile devices have multiple sensors and communication interfaces to derive proximity from.
- Only a subset of them is widely spread now or will be in future.

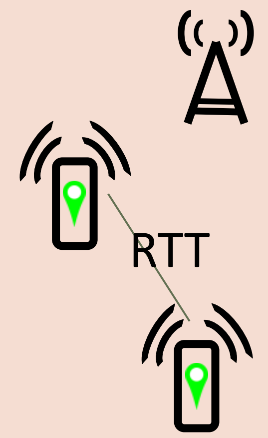
Most promising are:

1. Wi-Fi (especially Wi-Fi 6)
2. Ultra-Wideband (UWB)
3. Sound (Microphone, Speakers)
4. 5G Mobile Networks

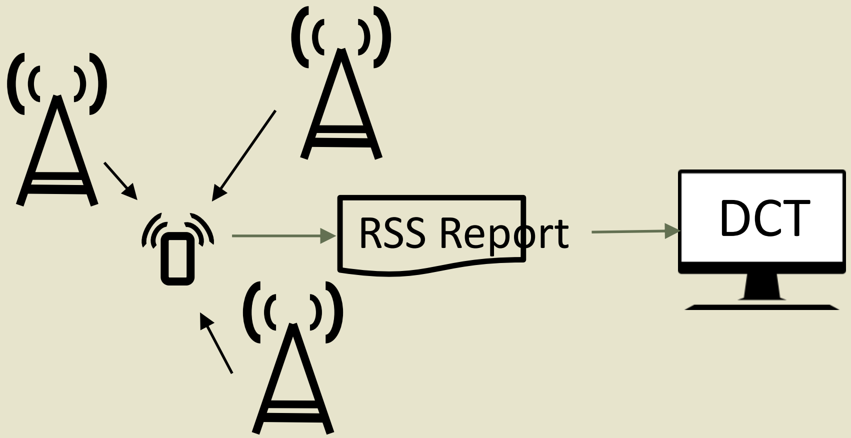
4G – Promising technologies for next-gen MCTA
Wi-Fi

WiFi - Multiple Solutions possible:

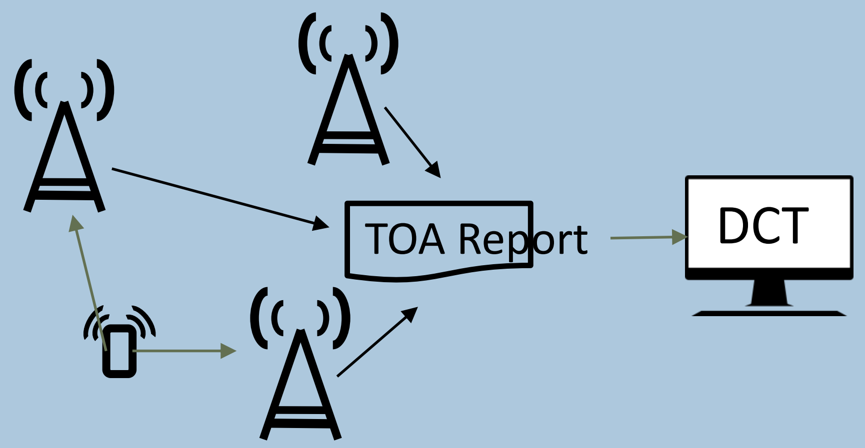
- Using Device-to-Device Signal Strength (RSS) like BLE
- Using Device-to-Device RTT (Round-Trip-Time)
- Differential RSS Fingerprinting: Comparison of RSS Fingerprints of surrounding Wi-Fi Stations
- Differential TOA Approach: Using Time-based Reports in Wi-Fi 6



Sidelink Ranging
RSS or RTT (Wi-Fi 6)



Differential RSS Fingerprinting:
Comparing RSS of surrounding stations



Differential TOA Approach:
Using Time-based Reports in Wi-Fi 6

4G – Promising technologies for next-gen MCTA
UWB

UWB

- Device to Device Ranging
  (Two-Way Ranging, Measurement of Round-Trip-Time RTT)
- Accuracy ~0.1-0.3 m

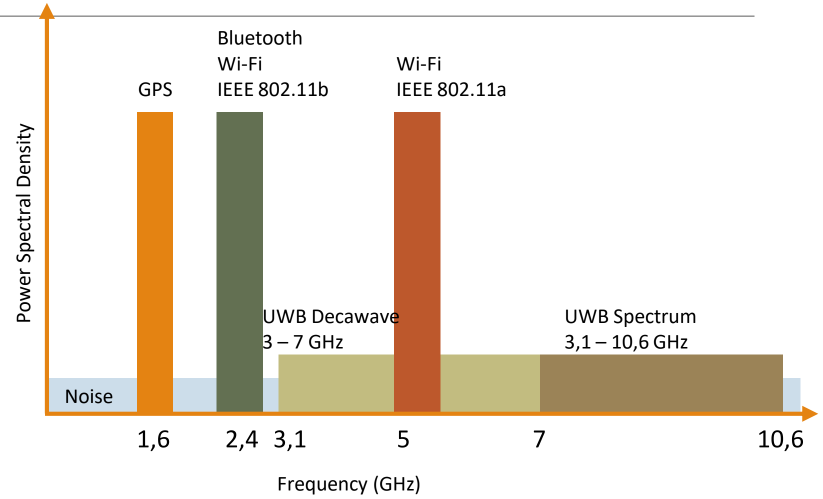
Pro:

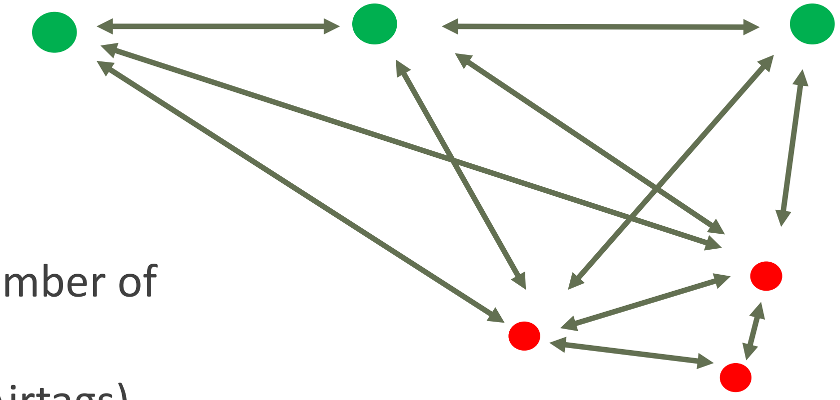
- High Accuracy
- Good approximation of distance based risk

Con:

- Scalability Limited (UWB only approach) due to high usage of bandwith)
- Energy consuming
- Up to now only a limited number of handsets support UWB

Option: UWB+BLE (like Apple Airtags)





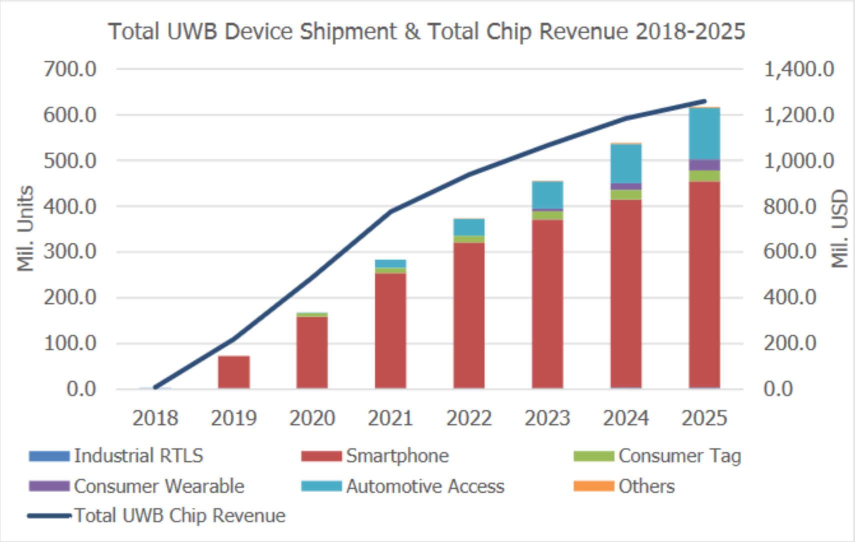
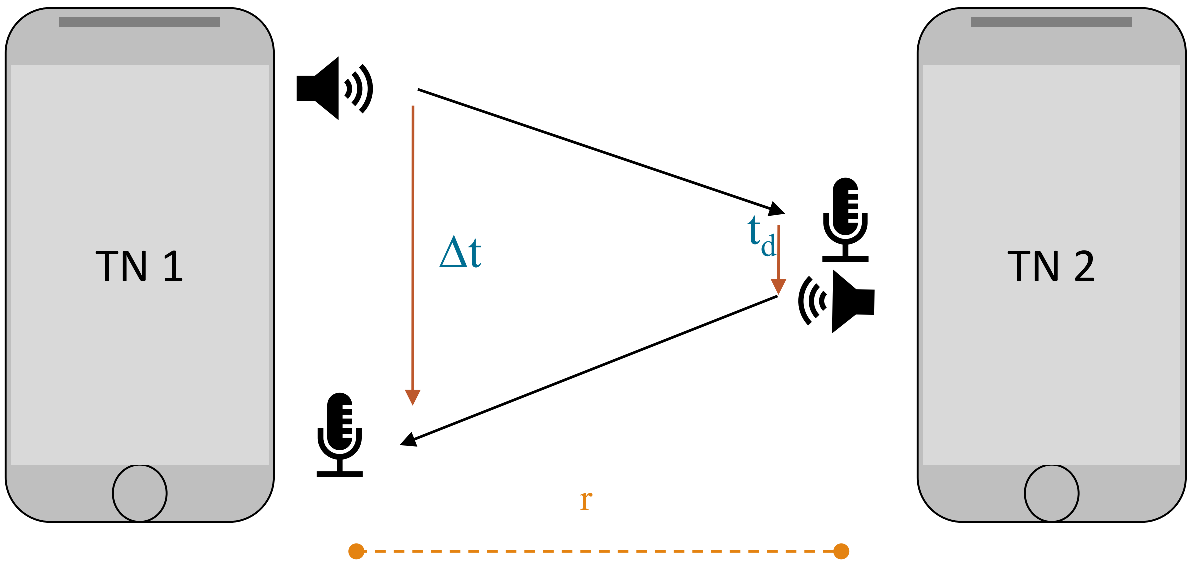


Figure 3 Device shipment and chip revenue, Source TSR Report, May 2020

4G – Promising technologies for next-gen MCTA
Ultrasound

Ultrasound/ultra sonic

- RTT and TOA with Radio Signal as Time Reference
- Using microphone and speaker
- Ultra sonic frequencies available in almost all smartphone devices
- Calculate distance *r* with runtime *Δt* and speed of sound c_s ($r = c_s * \Delta t$)
- Round Trip Time, RTT
- There and back (=> factor 0,5)
- No synchronization necessary



Performance:

- Experimental setup shows accuracy of < 40 cm on standard smartphone

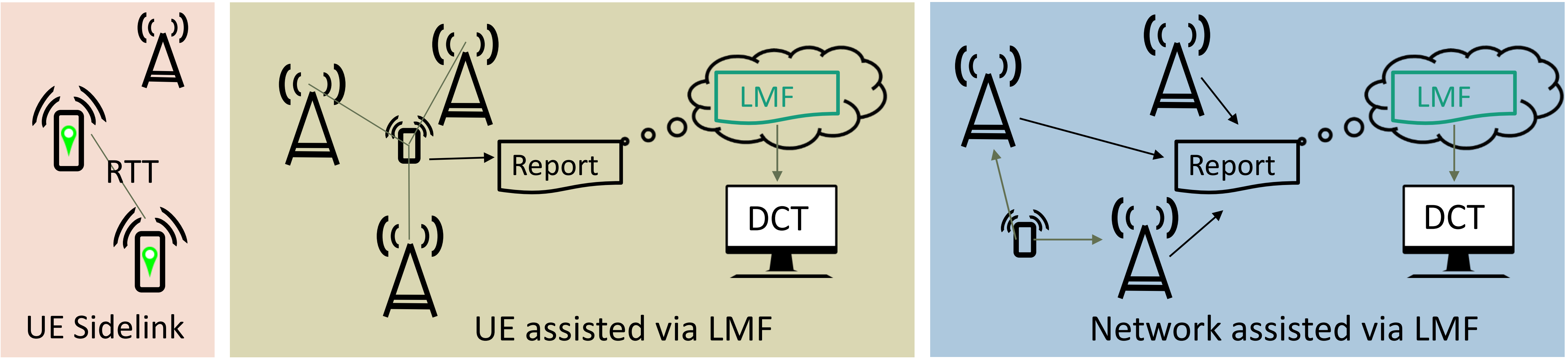
Privacy:

- Using the Microphone may be considered Privacy-Relevant

4G – Promising technologies for next-gen MCTA:
5G cellular networks

5G cellular networks

- Distance Estimation via Sidelink (Distance Estimation via Round-Trip-Time on "Device to Device" Signals)
  - Distance estimation device to device
- Using 5G Positioning in LMF (Location Management Function)
  - Using LMF as a trusted Unit and Anonymization
  - Contact tracing in the backend (core network)



UE: User Equipment | RTT: Round-Trip-Time | LMF: Location Management Function | DCT: Digital Contact Tracing

Thank you! Questions?

Christos Laoudias
KIOS Center of Excellence
University of Cyprus
Nicosia, Cyprus
laoudias@ucy.ac.cy

Steffen Meyer
Precise Positioning and Analytics Department
Fraunhofer Institute of Integrated Circuits
Nuremberg, Germany
steffen.meyer@iis.fraunhofer.de

Philippos Isaia
KIOS Center of Excellence
University of Cyprus
Nicosia, Cyprus
Isaia.philippos@ucy.ac.cy

Thomas Windisch
Precise Positioning and Analytics Department
Fraunhofer Institute of Integrated Circuits
Nuremberg, Germany
thomas.windisch@iis.fraunhofer.de

Justus Benzler
Robert Koch Institute
Berlin, Germany
BenzlerJ@rki.de

Maximilian Lenkeit
SAP SE
Technology & Innovation
Walldorf, Germany
maximilian.lenkeit@sap.com