

Automated Analysis of Exposure Notification Systems

CISPA Helmholtz Center for Information Security

Kevin Morio, Ilkan Esiyok, Dennis Jackson, Robert Künnemann
USENIX Security '23 | August 11, 2023





The Beginning

UK EDITION

INDEPENDENT

NEWS SPORT VOICES CULTURE LIFESTYLE TRAVEL PREMIUM MORE

Women's World ... Galaxy: The R

News > World > Asia

Nearly 30 people struck by outbreak of mystery illness in Chinese city

Experts suspect link to seafood market, but residents fear return of Sars epidemic that killed nearly 800 people.

Jane Dalton • Tuesday 31 December 2019 14:57 • [1](#) Comments

Health chiefs in **China** are investigating an outbreak of a respiratory illness that some people have likened to the 2003 **Sars** epidemic that killed nearly 800 people.

Doctors say 27 people have fallen ill in December with a suspected strain of viral **pneumonia**, seven of whom are in serious condition.

Most of the sick had visited a **seafood** market in the central city of **Wuhan**, and experts are investigating whether the disease is linked to it.

"The cause of the disease is not clear," the official *People's Daily* newspaper posted online, citing hospital officials. "We cannot confirm it is what's being spread online, that it is the Sars virus. Other severe pneumonia is more likely."

Experts from the National Health Commission travelled to Wuhan to lead the investigation into the disease, state television reported.

Doctors have yet to identify the virus responsible but initial laboratory tests showed that the cases were viral pneumonia and had not spread from person to person, according to the Wuhan health commission.

Patients were isolated and their close contacts were under medical observation. An investigation and clean-up were under way at the seafood market, the commission said.

Subscribe Latest Issues

SCIENTIFIC AMERICAN. Sign In | Newsletters

COVID Health Mind & Brain Environment Technology Space & Physics Video Podcasts Opinion


STAT

PUBLIC HEALTH

Cause of Wuhan's Mysterious Pneumonia Cases Still Unknown, Chinese Officials Say

The virus has sickened 59 people so far but does not appear to be transmitting among humans

By Helen Branswell, STAT on January 6, 2020



Credit: Getty Images

THE NEW CORONAVIRUS OUTBREAK: WHAT WE KNOW SO FAR

PUBLIC HEALTH
How China's 'Bat Woman' Hunted Down Viruses from SARS to the New Coronavirus
Jane Qiu

PUBLIC HEALTH
WHO Declares the Coronavirus Outbreak a Pandemic
Helen Branswell, Andrew Joseph and STAT

PUBLIC HEALTH
Preparing for Coronavirus to Strike the U.S.
Zeynep Tufekci

The cause of mysterious pneumonia cases in the Chinese city of Wuhan



The Beginning

UK EDITION

INDEPENDENT

NEWS SPORT VOICES CULTURE LIFESTYLE TRAVEL

News > World > Asia

Nearly 30 people of mystery illness

Experts suspect link to seafood market, but

Jane Dalton • Tuesday 31 December 2019 14:57

Health chiefs in **China** are investigating an illness that some people have likened to the illness that killed nearly 800 people.

Doctors say 27 people have fallen ill in **Denmark** of viral **pneumonia**, seven of whom are in **Denmark**.

Most of the sick had visited a **seafood** market and experts are investigating whether the illness is what's being spread online, that it is the **pneumonia** is more likely."

"The cause of the disease is not clear," the newspaper posted online, citing hospital records. "The cause of the disease is not clear," the newspaper posted online, citing hospital records. "The cause of the disease is not clear," the newspaper posted online, citing hospital records.

Experts from the National Health Commission are investigating the disease, state officials said.

Doctors have yet to identify the virus. The tests showed that the cases were viral and spread from person to person, according to the commission said.

Patients were isolated and their close contacts were under observation. An investigation and clinical trial at the market, the commission said.

World Health Organization

Search by Country, Territory, or Area

Global > Russian Federation

Overview Measures Table View Data More Resources

Cases - Total

- > 5,000,000
- 500,001 – 5,000,000
- 50,001 – 500,000
- 5,001 – 50,000
- 1 – 5,000
- 0
- Not applicable

2,985 new cases last 7 days

22,977,274 cumulative cases

399,854 cumulative deaths

Download Map Data

In **Russian Federation**, from **3 January 2020** to **1:56pm CEST, 2 August 2023**, there have been **22,977,274 confirmed cases** of COVID-19 with **399,854 deaths**, reported to WHO. As of **5 July 2023**, a total of **186,692,479 vaccine doses** have been administered.

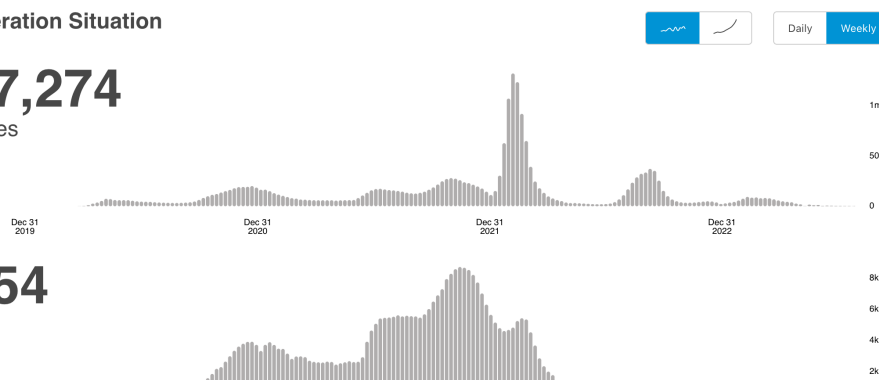
Russian Federation Situation

22,977,274

confirmed cases

399,854

deaths



Subscribe Latest Issues

SCIENTIFIC AMERICAN

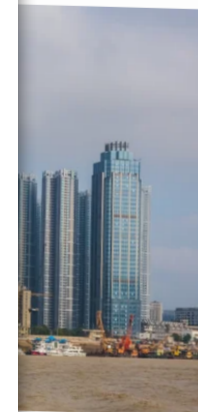
Sign In | Newsletters

Technology Space & Physics Video Podcasts Opinion

China's Mysterious Illness Still Unknown, Officials Say

It does not appear to be transmitting among humans

January 6, 2020



THE NEW CORONAVIRUS OUTBREAK: WHAT WE KNOW SO FAR

PUBLIC HEALTH

How China's 'Bat Woman' Hunted Down Viruses from SARS to the New Coronavirus

Jane Qiu

PUBLIC HEALTH

WHO Declares the Coronavirus Outbreak a Pandemic

Helen Branswell, Andrew Joseph and STAT

PUBLIC HEALTH

Preparing for Coronavirus to Strike the U.S.

Zeynep Tufekci

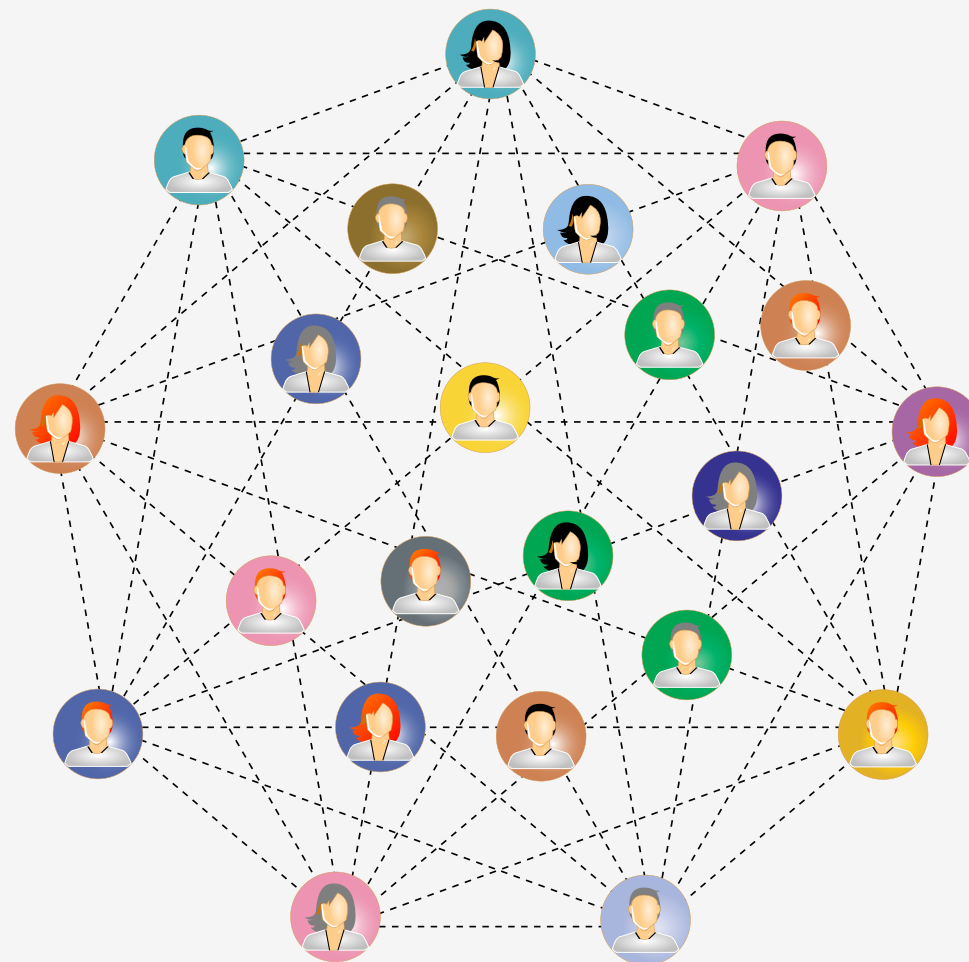


Contact Tracing



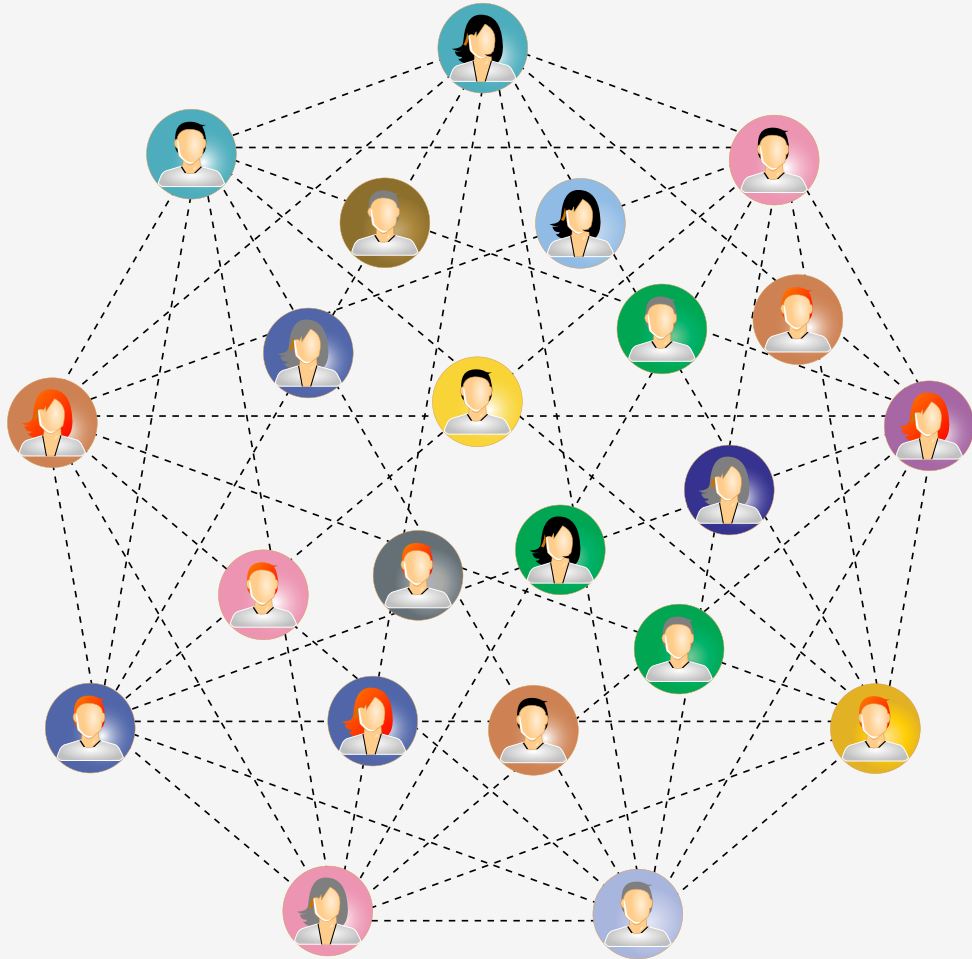
Contact tracing can break the chains of transmission through the rapid identification, isolation and clinical care of cases, and providing supported quarantine of contacts, meaning that virus transmission can be stopped.

WHO





Exposure Notification Systems



The aim of an **exposure notification system (ENS)** is to notify users who may have been exposed to a disease by being in contact with an infected person.



Research Questions

RQ1: How to formalize key security properties of ENS?

RQ2: What attacks are possible?

RQ3: What is the maximum impact of the attacks?



Analyzed ENS



ROBust and privacy-pres**ER**ving proximity **T**racing | **ROBERT**

PRIVATICS team, Inria and Fraunhofer AISEC

+60 million downloads



Decentralized **P**rivacy-**P**reserving **P**roximity **T**racing | **DP3T**

Troncoso et al.

Influenced the Google/Apple Exposure Notification System



Corona Warn-App | **CWA**

SAP and Deutsche Telekom

+48 million downloads

+208 million downloads (19 countries in EFGS)

Formally modeled
analyzed using



Tamarin Prover

ROBERT vs. DP3T

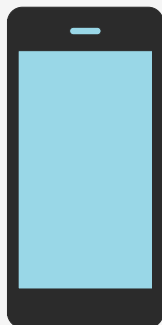
=



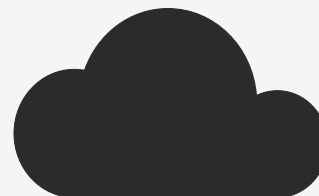


ROBERT | Registration

Phone



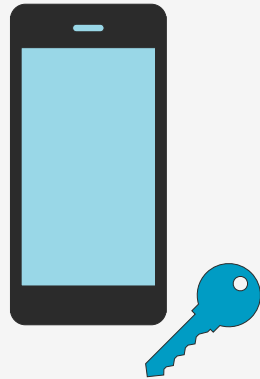
Back end





ROBERT | Registration

Phone

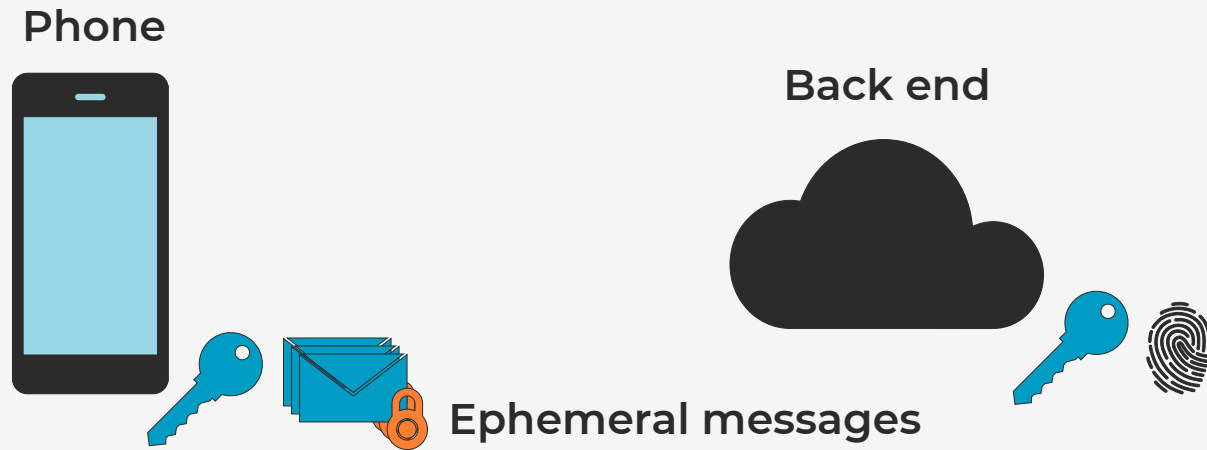


Back end



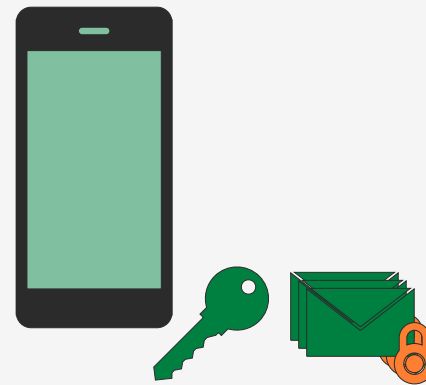


ROBERT | Registration



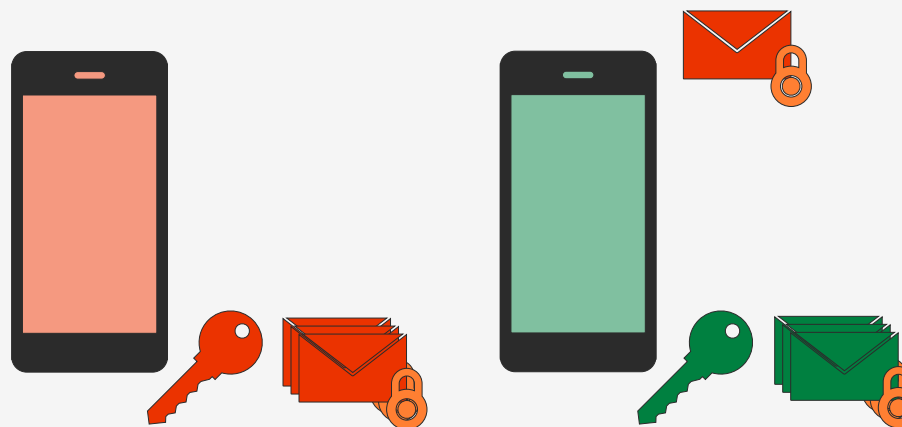
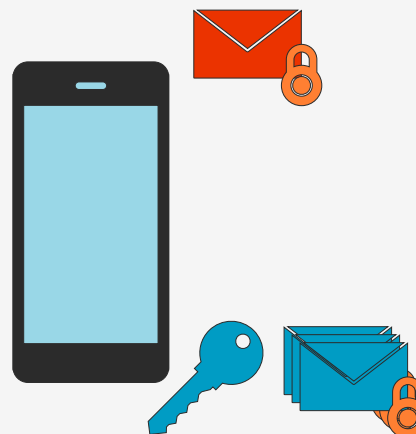


ROBERT | Exchange



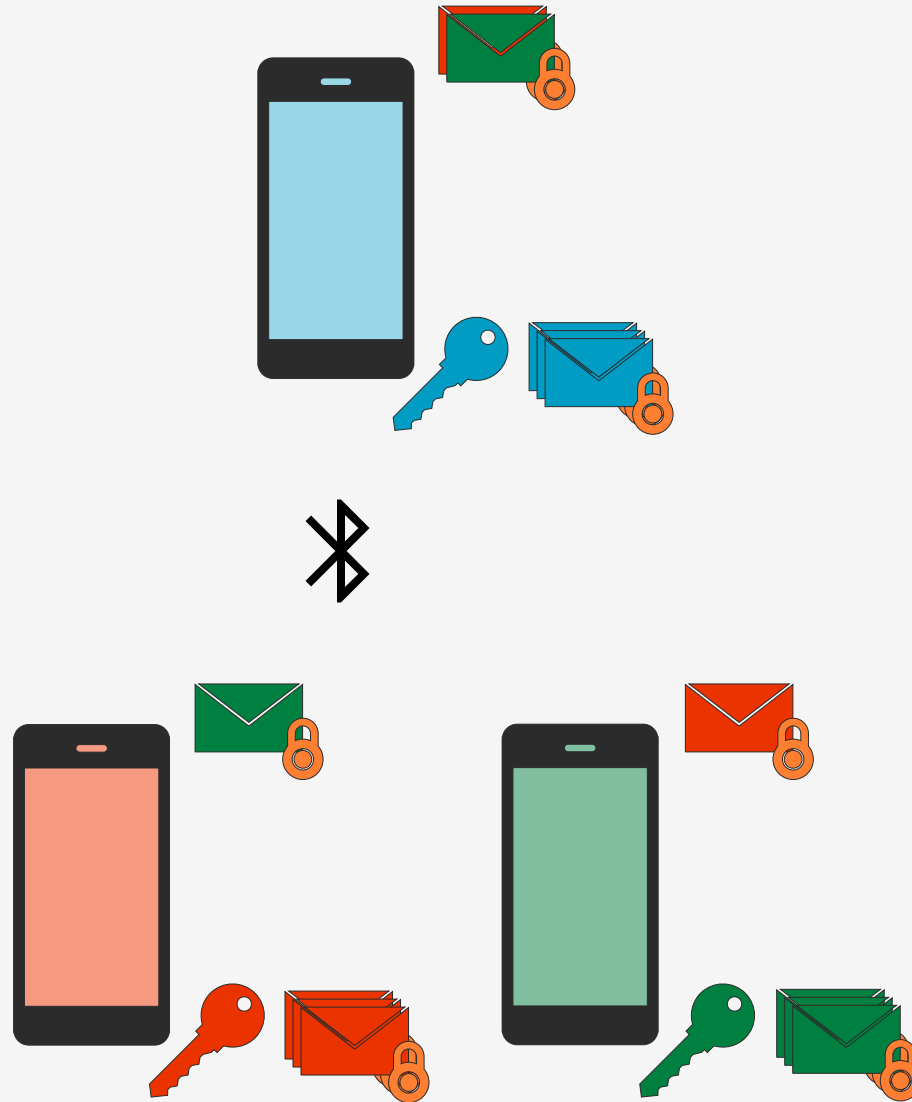


ROBERT | Exchange



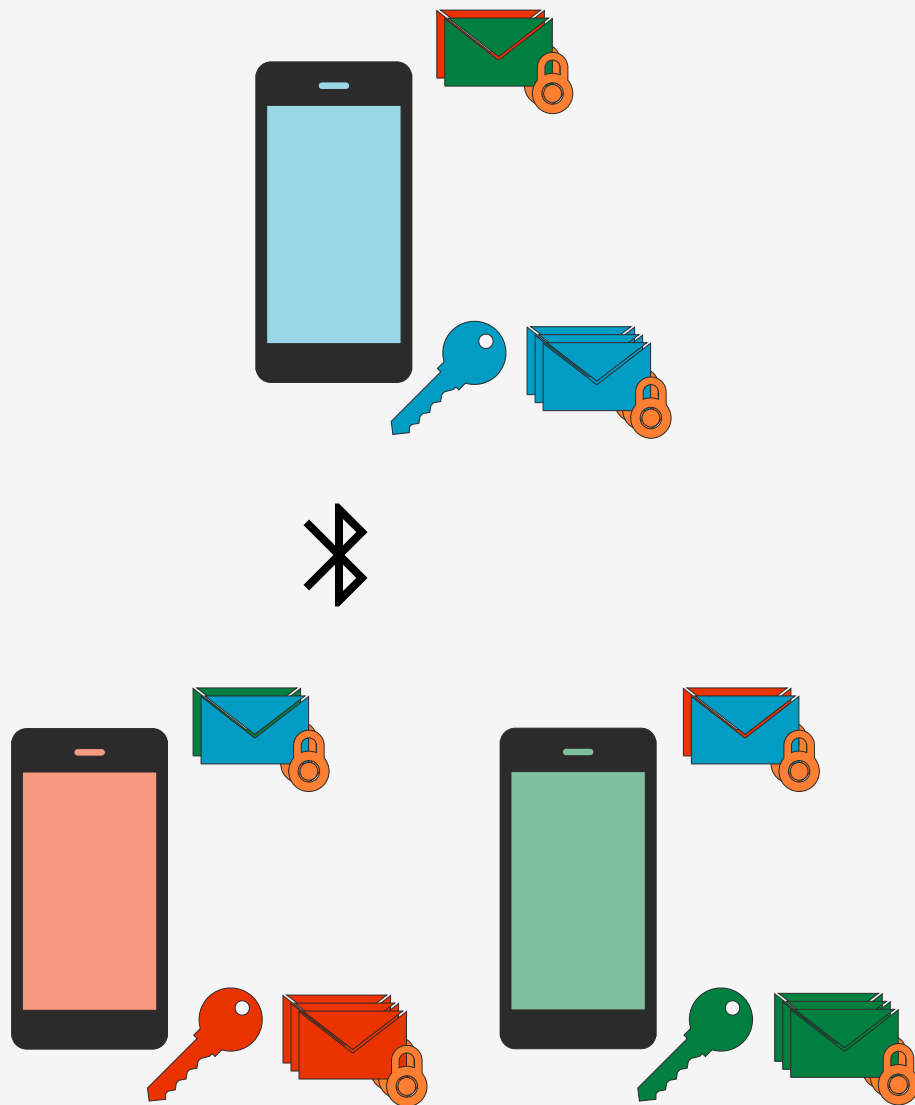


ROBERT | Exchange





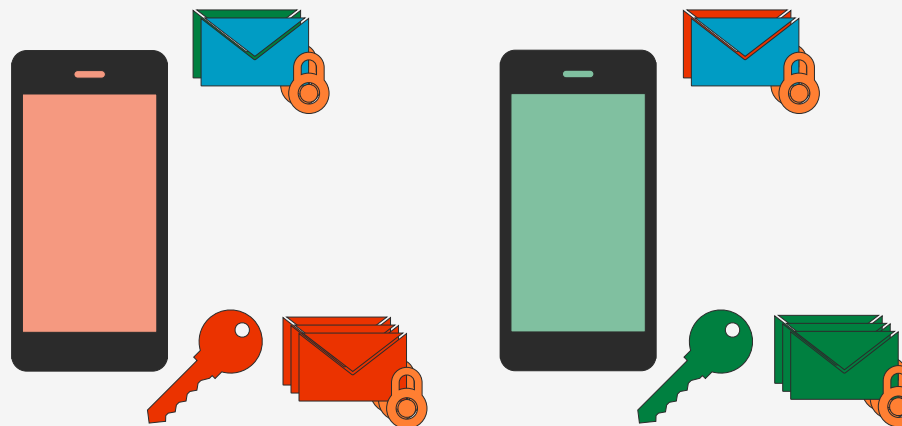
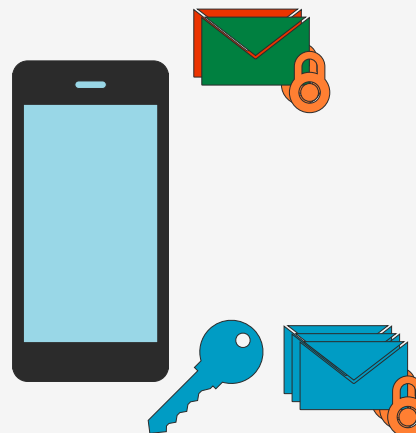
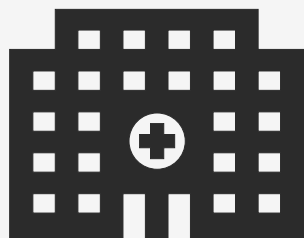
ROBERT | Exchange





ROBERT | Testing

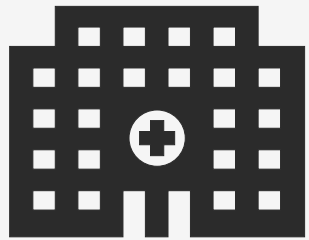
Health Authority



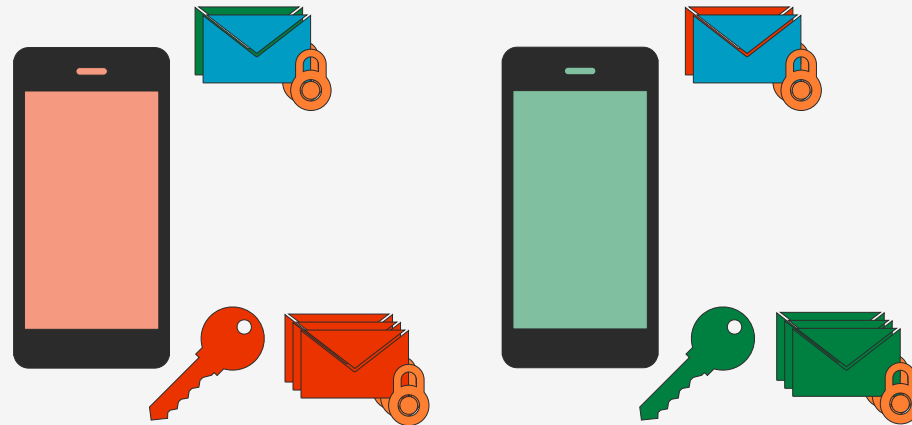
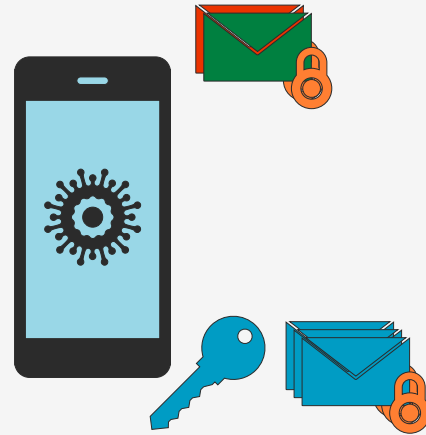


ROBERT | Testing

Health Authority



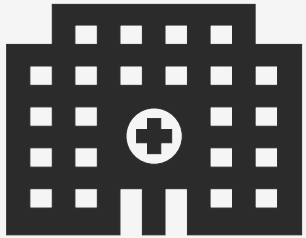
Positive



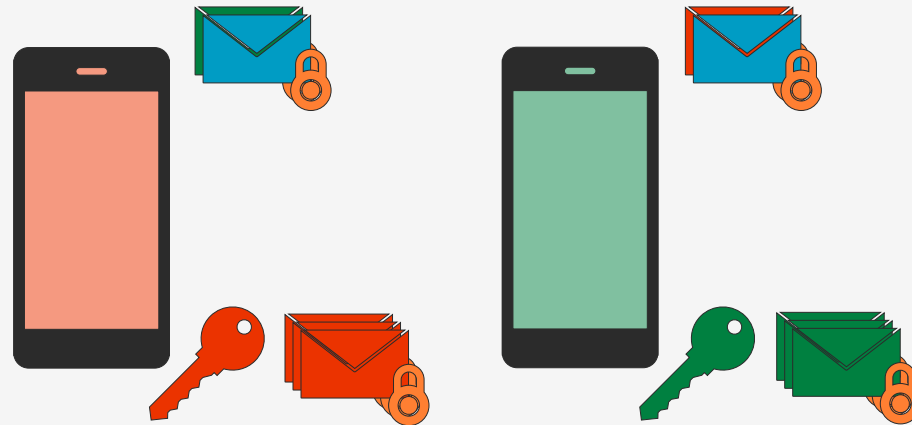


ROBERT | Testing

Health Authority



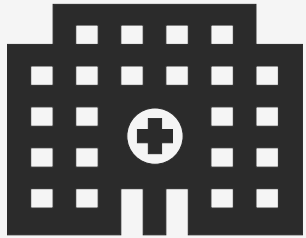
Positive





ROBERT | Uploading

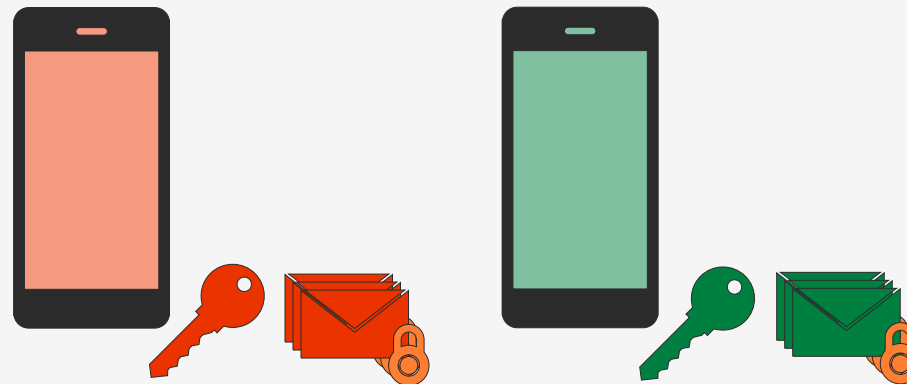
Health Authority



Positive



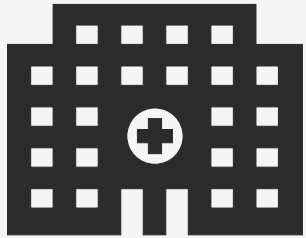
Back end



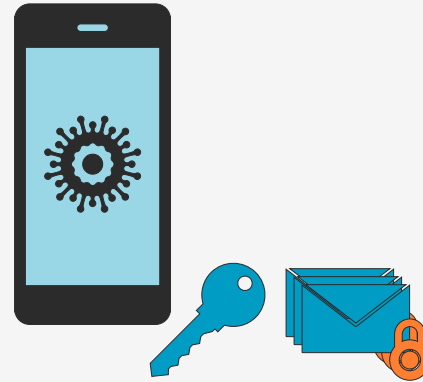


ROBERT | Uploading

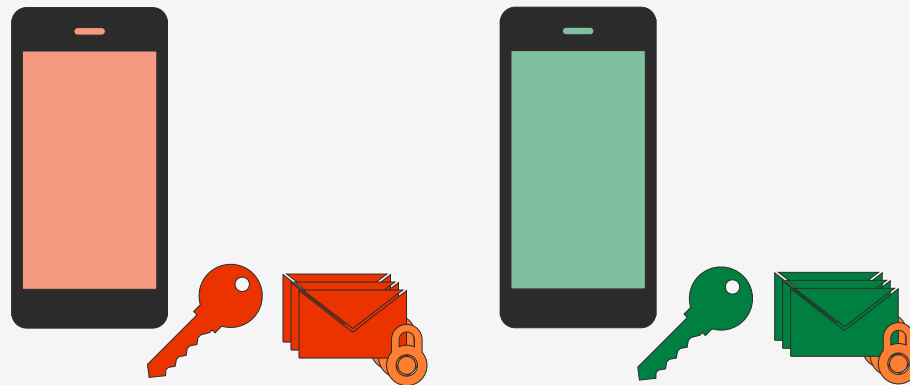
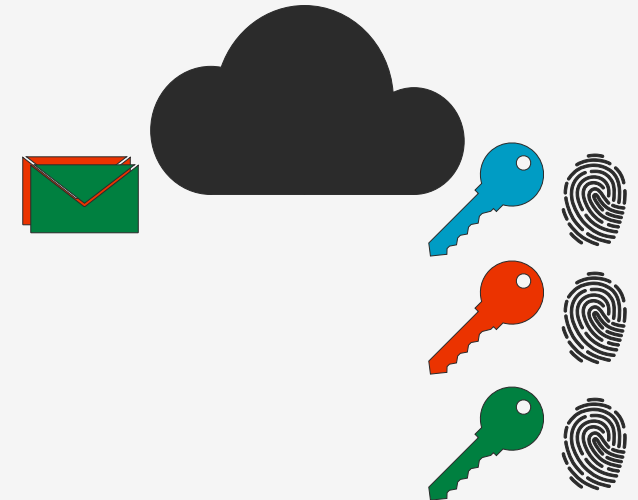
Health Authority



Positive



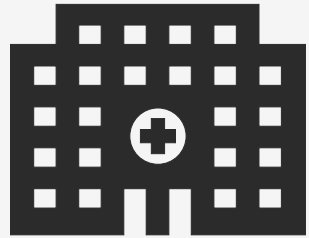
Back end



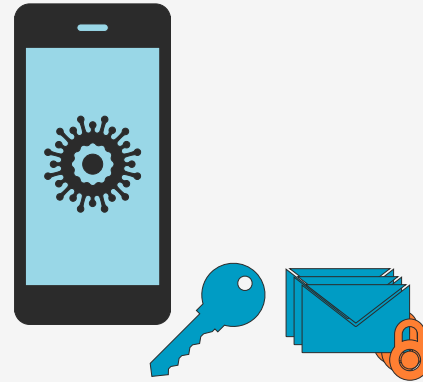


ROBERT | Uploading

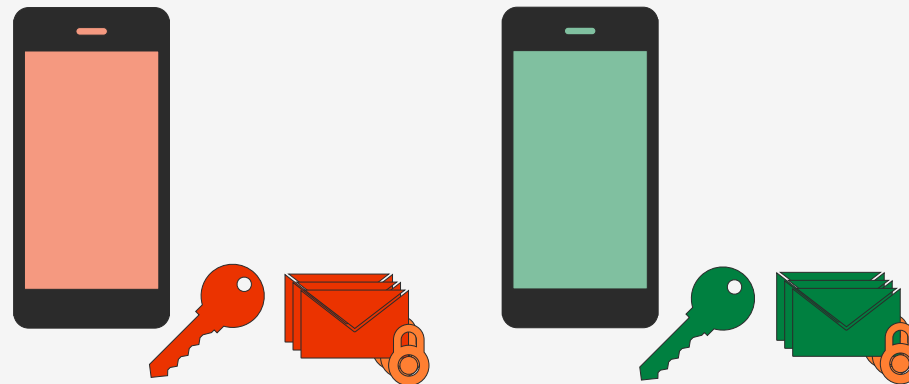
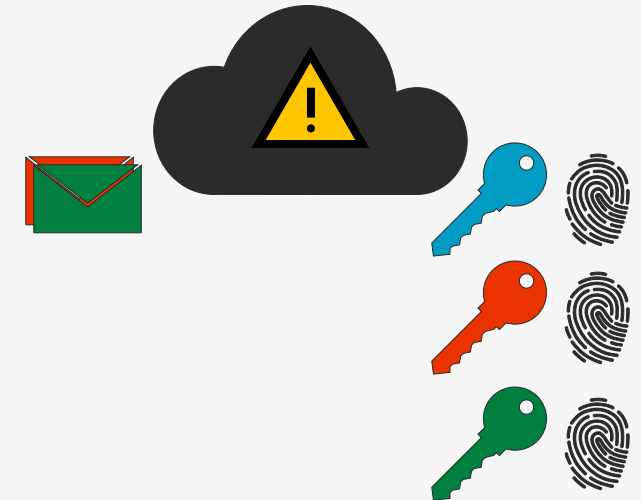
Health Authority



Positive



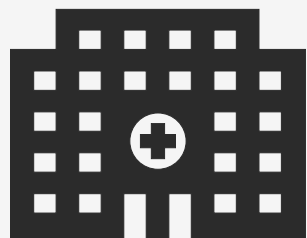
Back end





ROBERT | Uploading

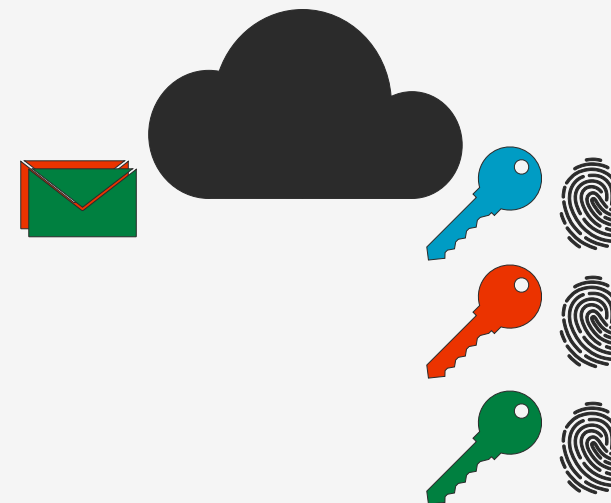
Health Authority



Positive



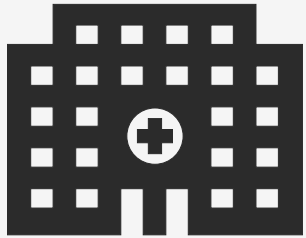
Back end



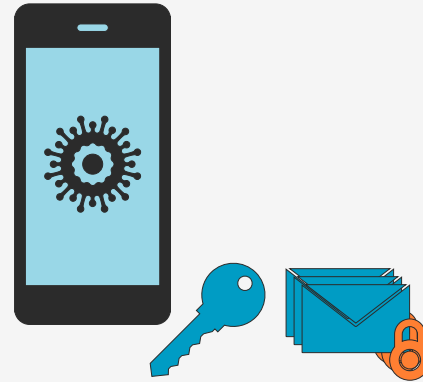


ROBERT | Uploading

Health Authority

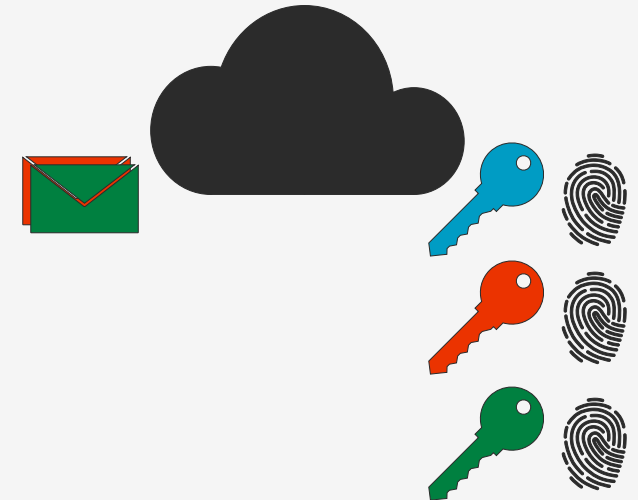


Positive



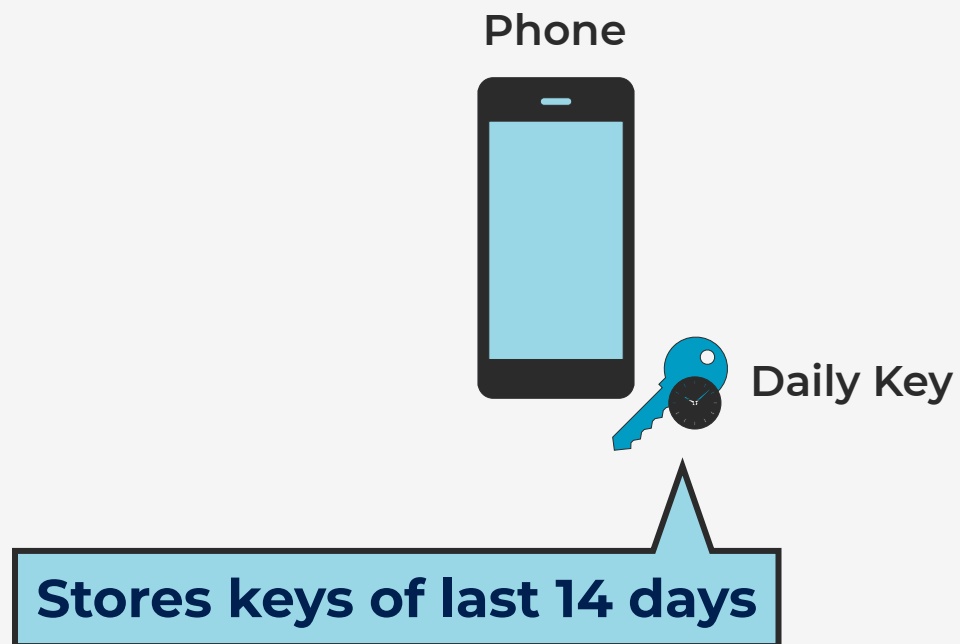
Centralized Setting

Back end



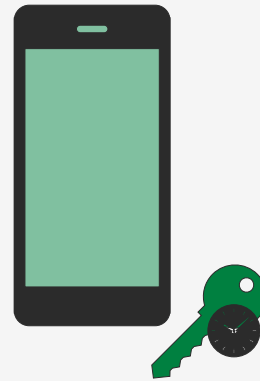
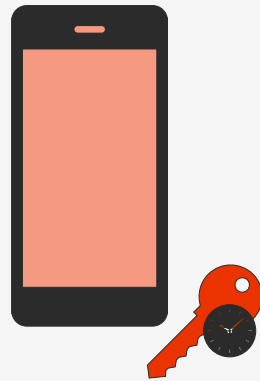
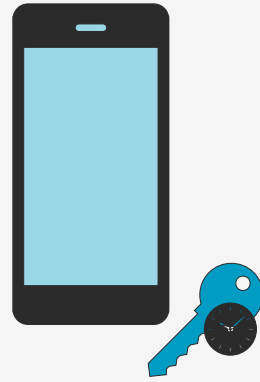


DP3T | Daily Key Generation



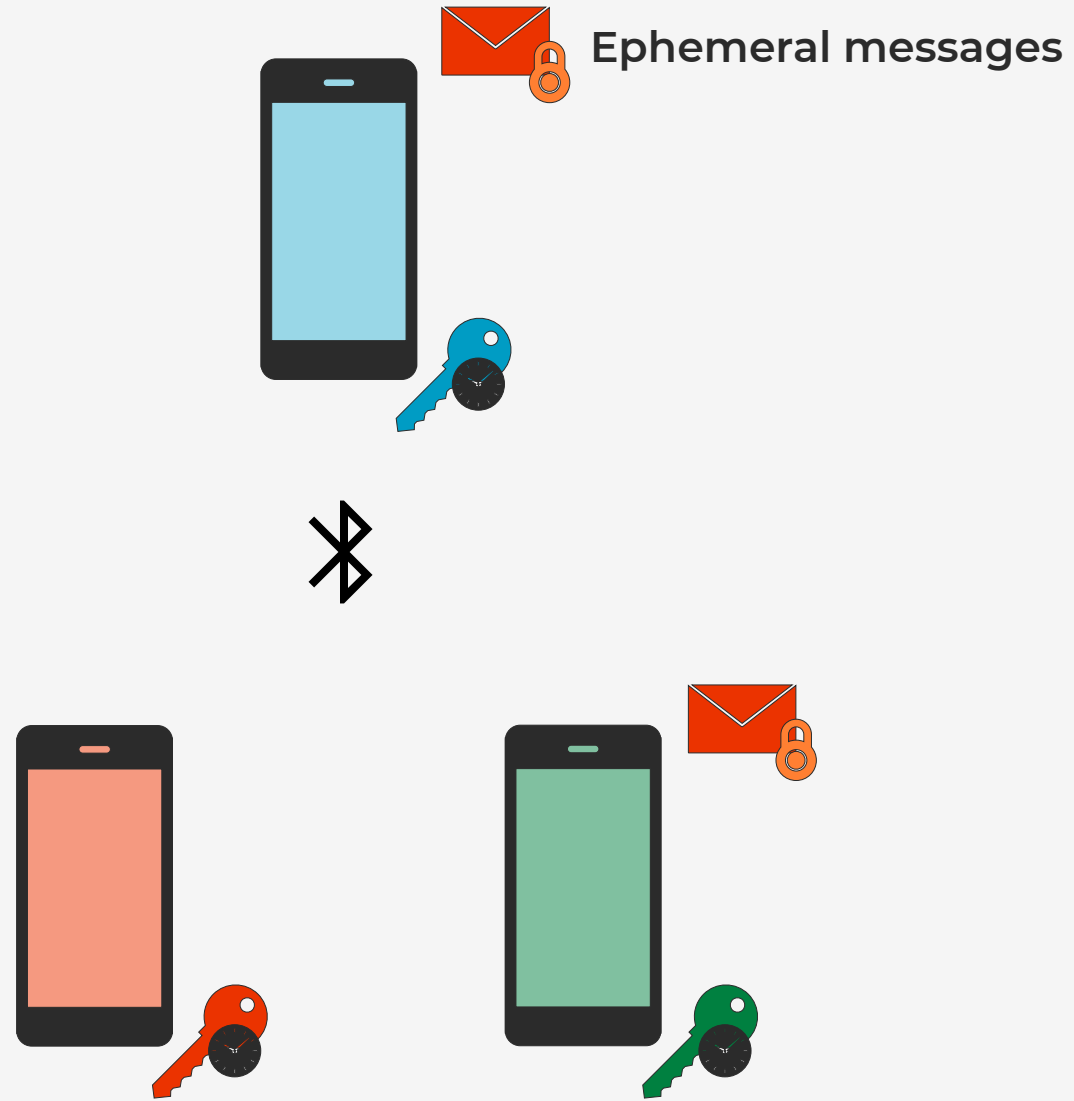


DP3T | Exchange



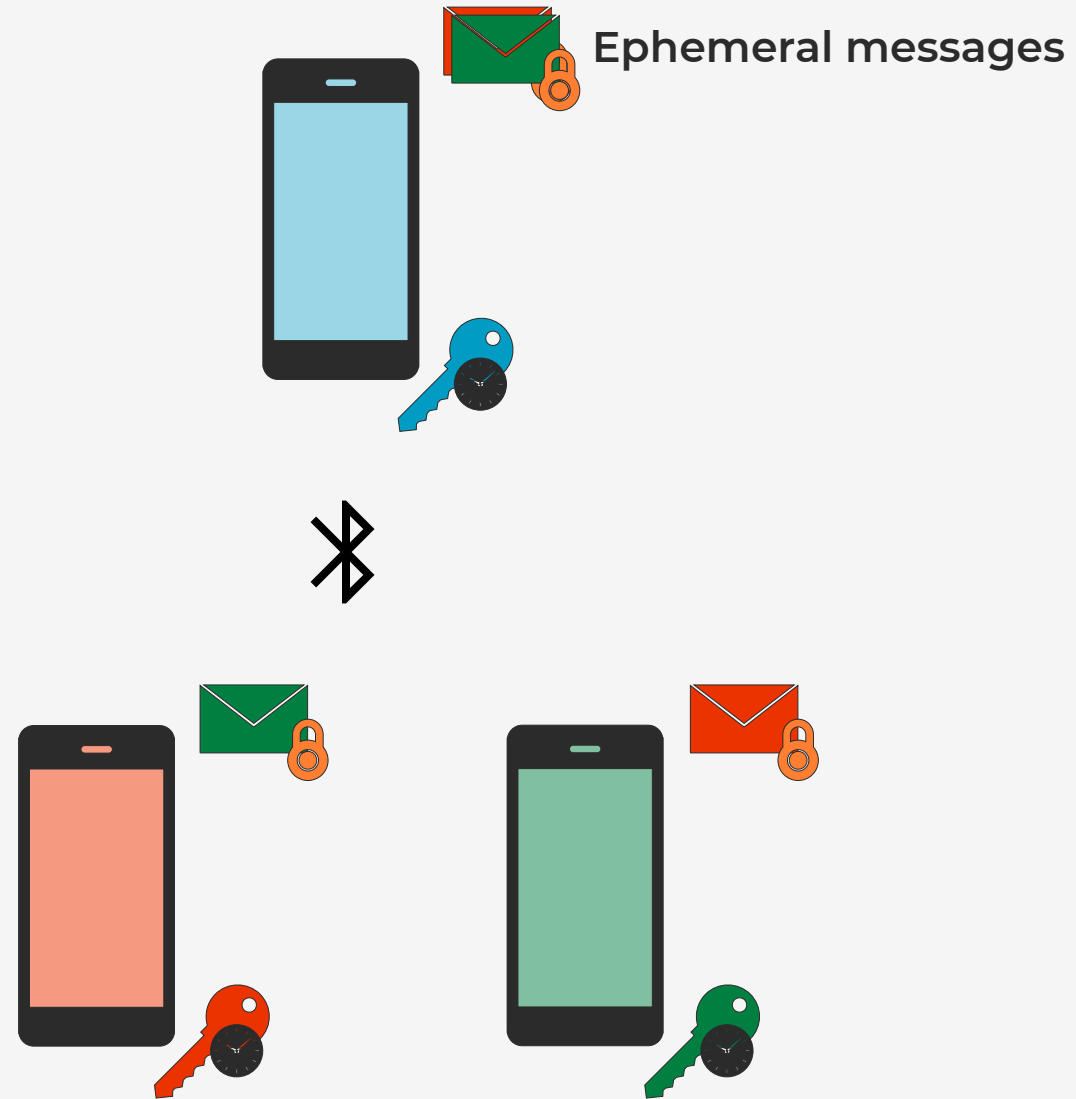


DP3T | Exchange



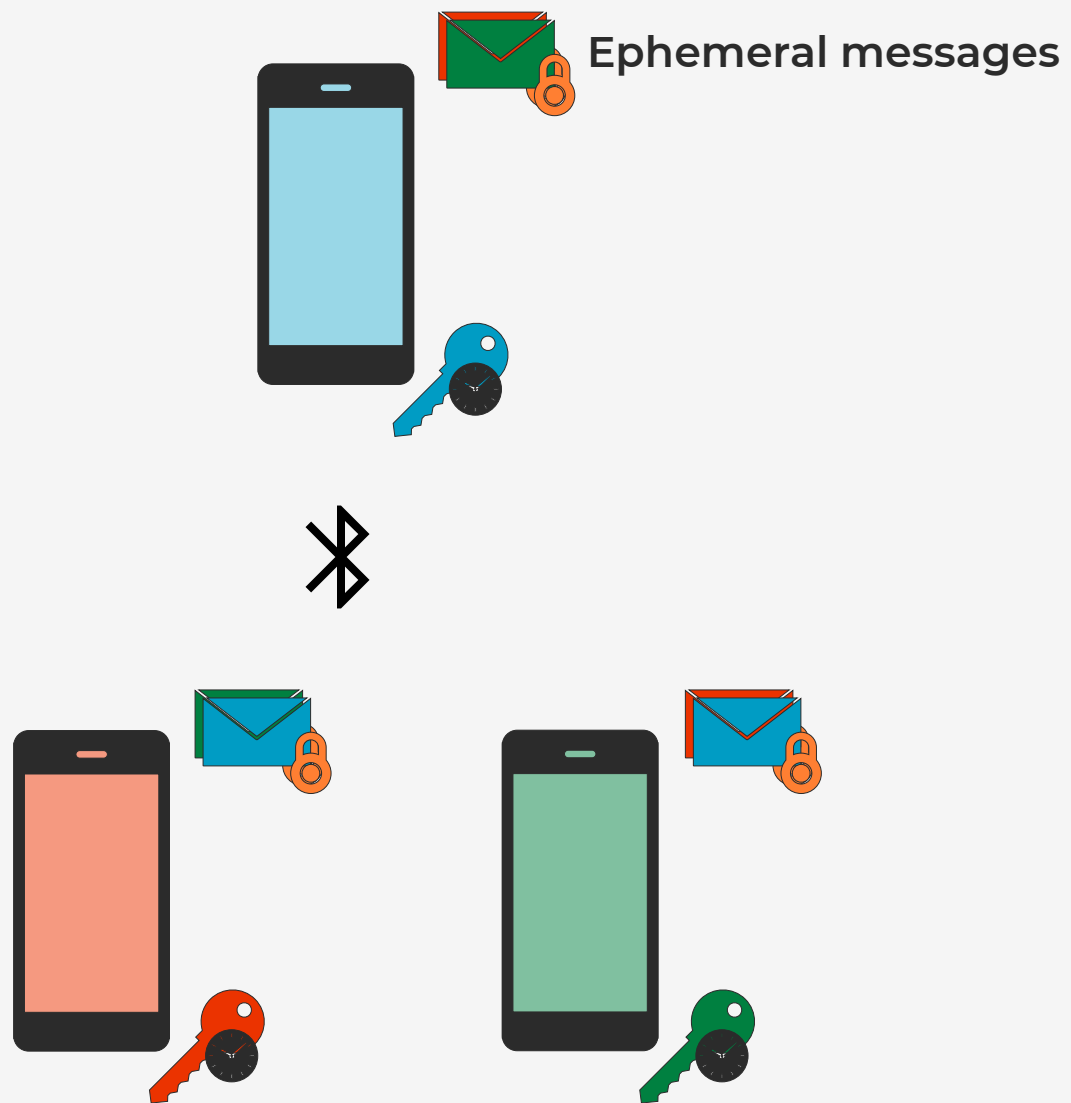


DP3T | Exchange





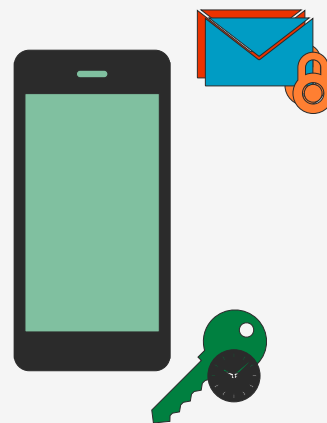
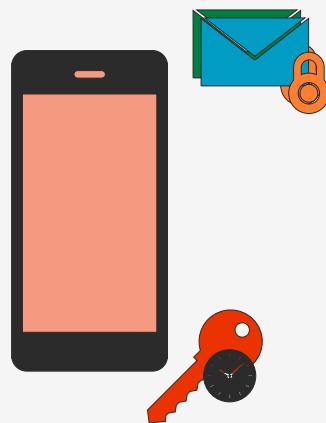
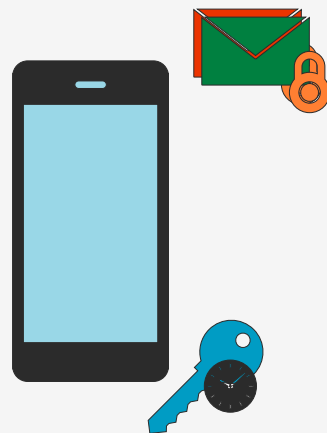
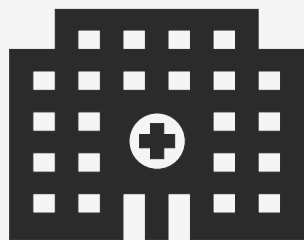
DP3T | Exchange





DP3T | Testing

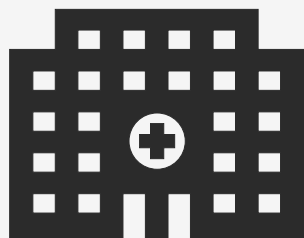
Health Authority



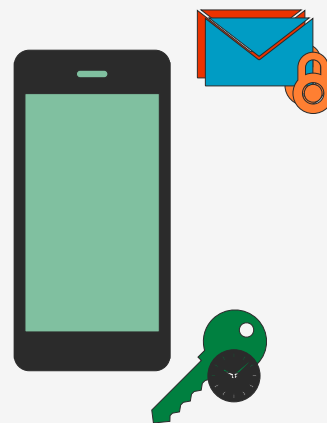
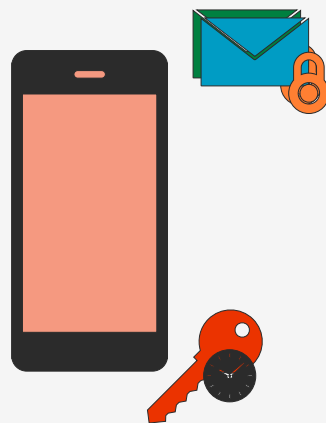
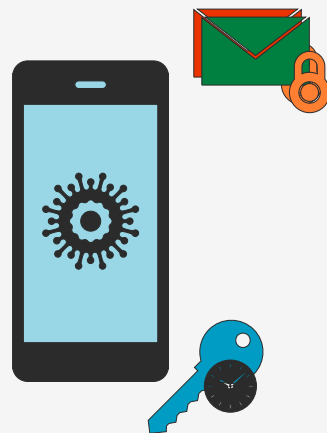


DP3T | Testing

Health Authority



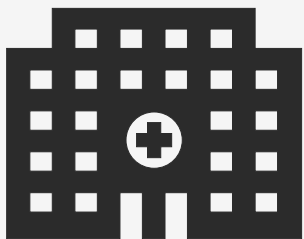
Positive



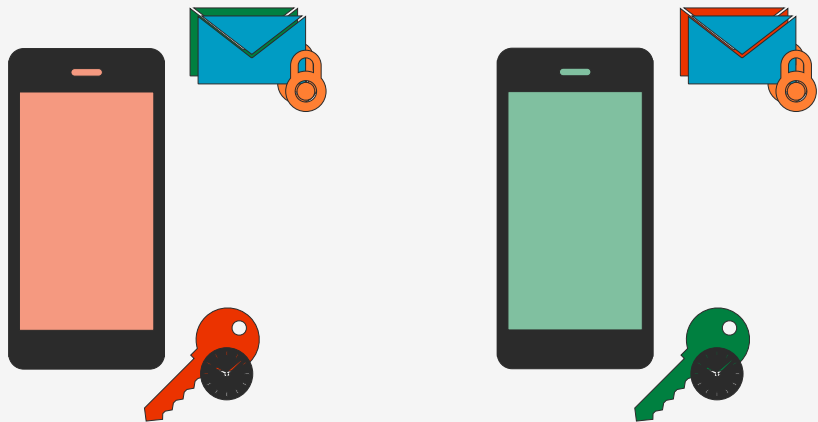
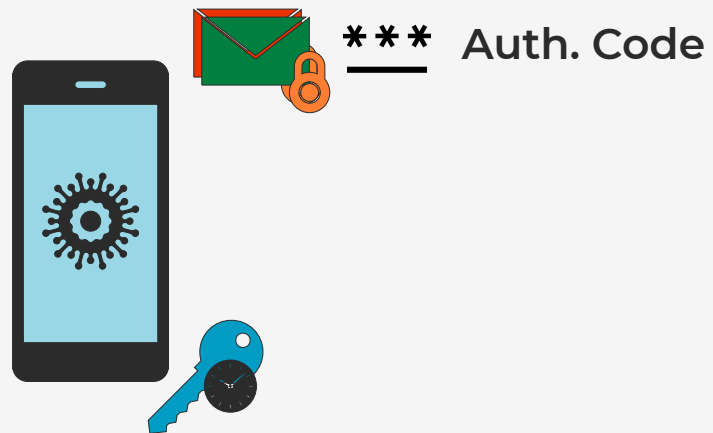


DP3T | Testing

Health Authority

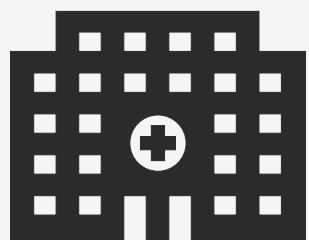


Positive

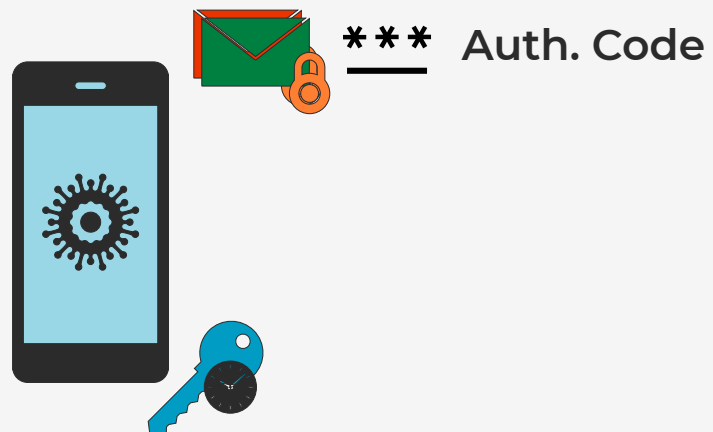




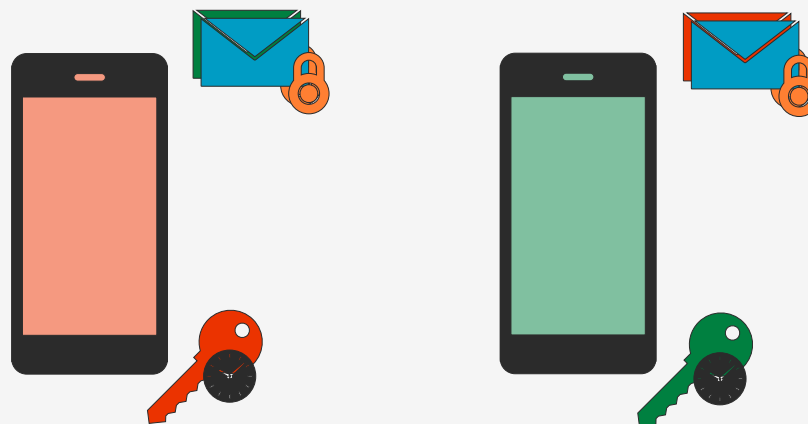
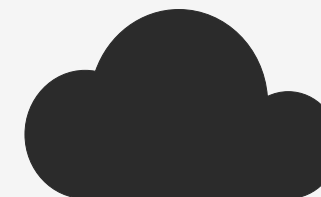
DP3T | Uploading



Positive

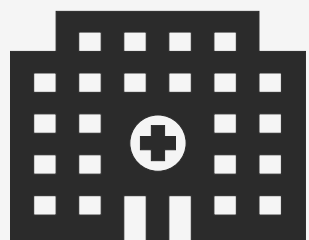


Back end

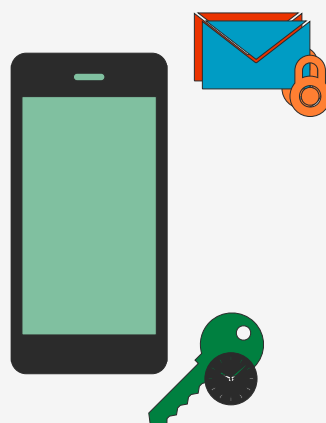
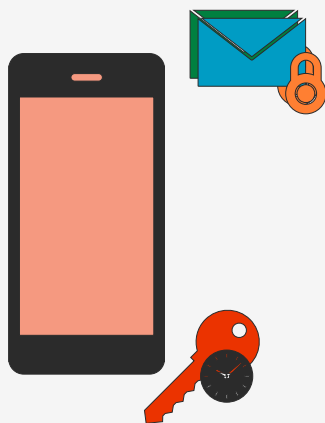
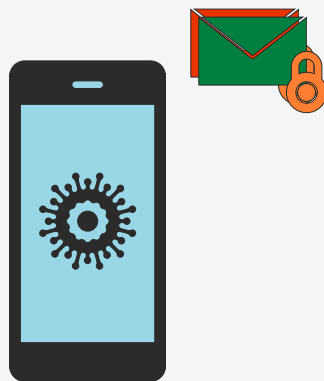




DP3T | Uploading



Positive

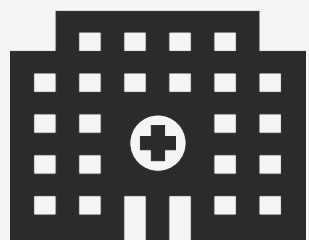


Back end

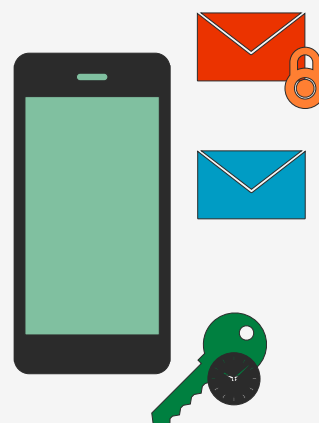
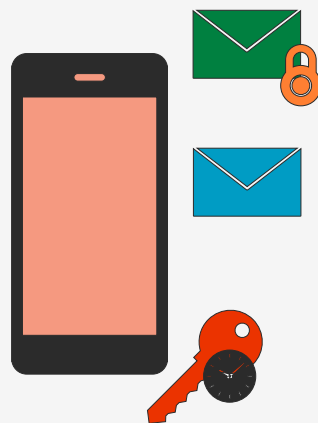
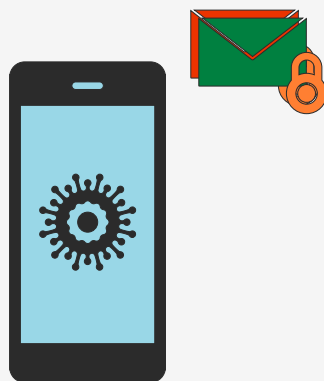




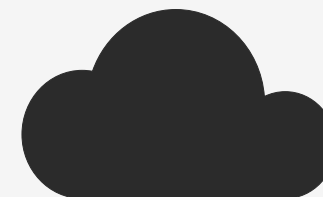
DP3T | Uploading



Positive

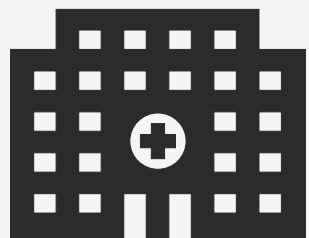
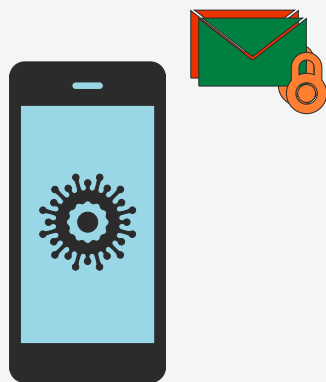


Back end



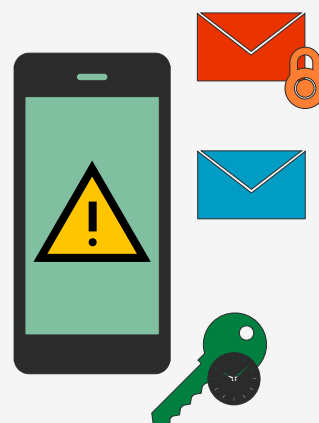
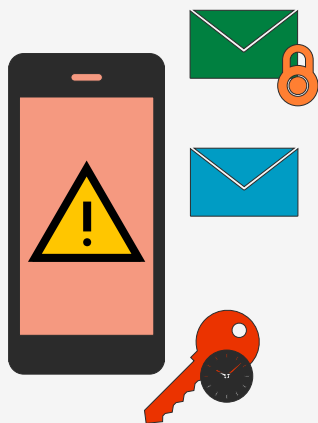
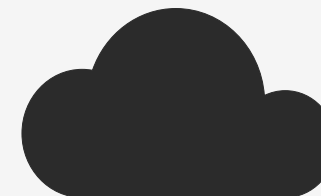


DP3T | Uploading



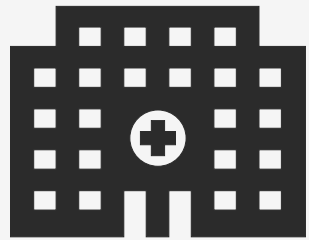
Positive

Back end





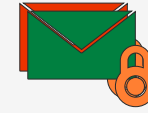
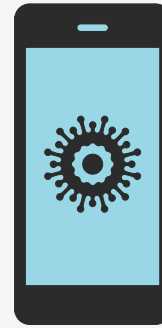
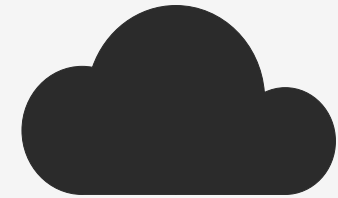
DP3T | Uploading



Positive

Decentralized Setting

Back end



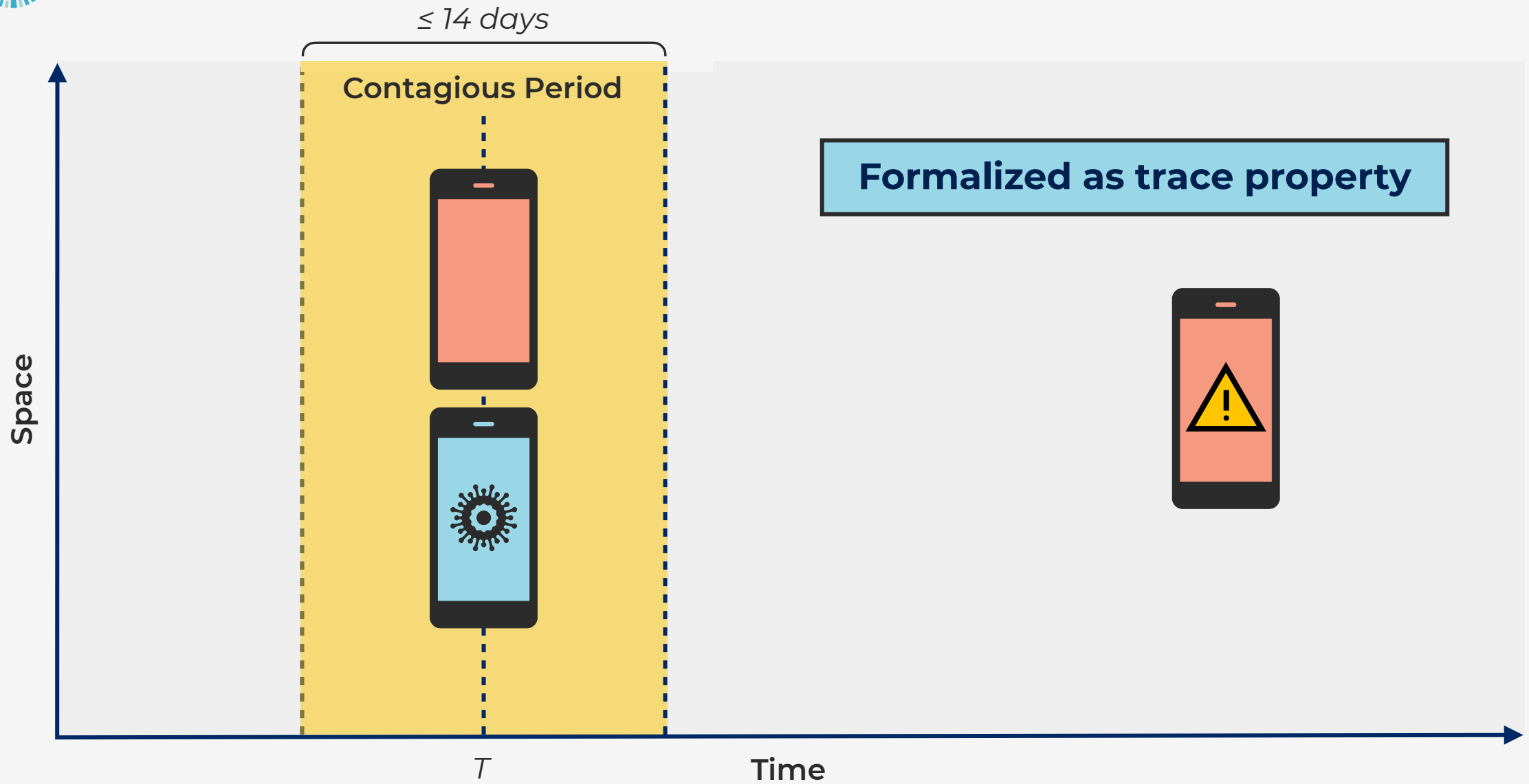
Security Properties

=





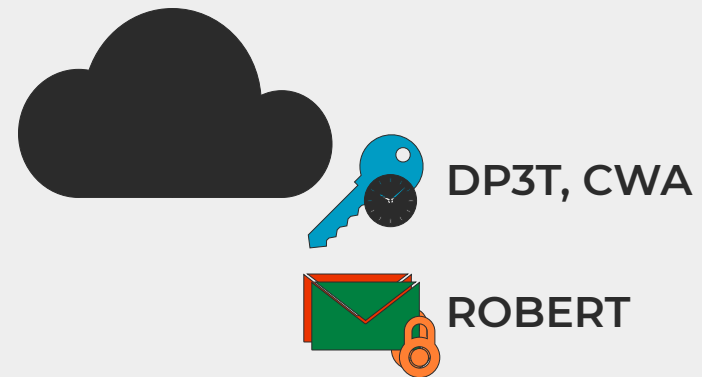
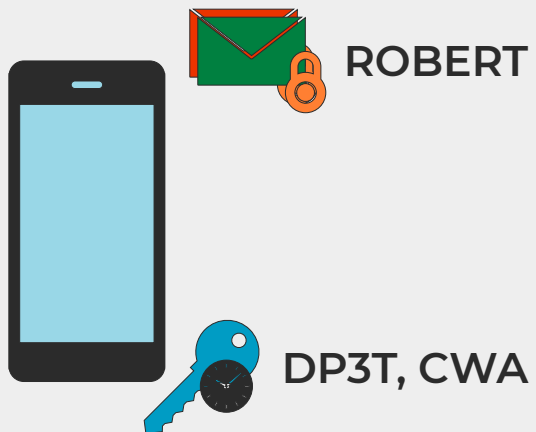
Soundness





Upload Authorization

Formalized as trace property



Time

Attacks

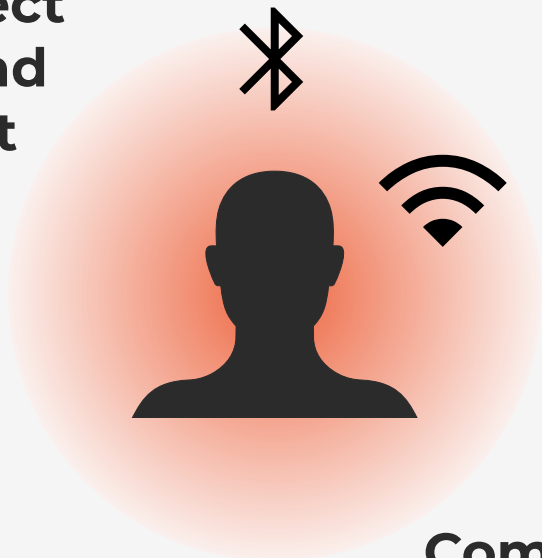
=





Attacker Model

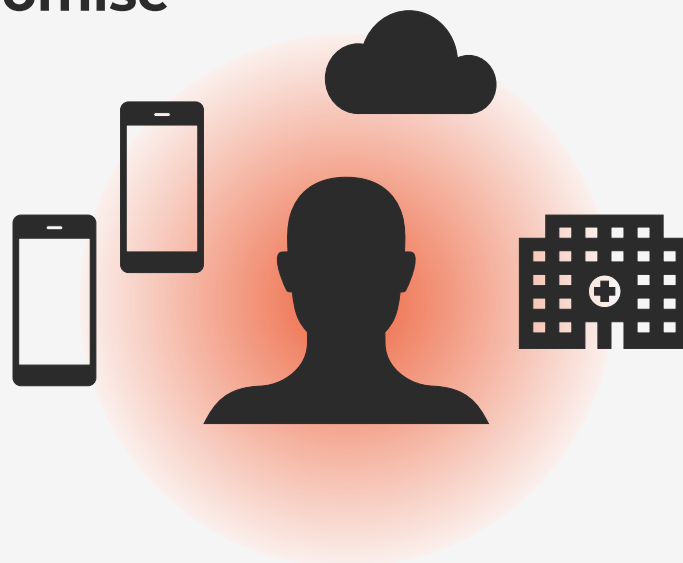
Inject
Read
Edit



Multi-locality



Compromise

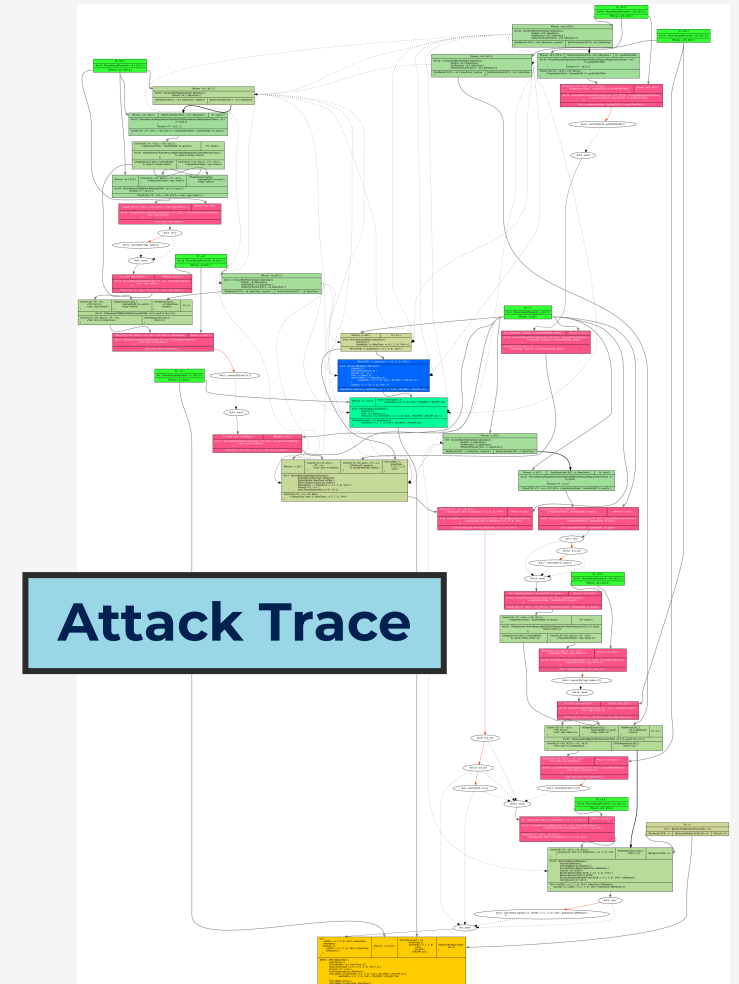




Attack Patterns

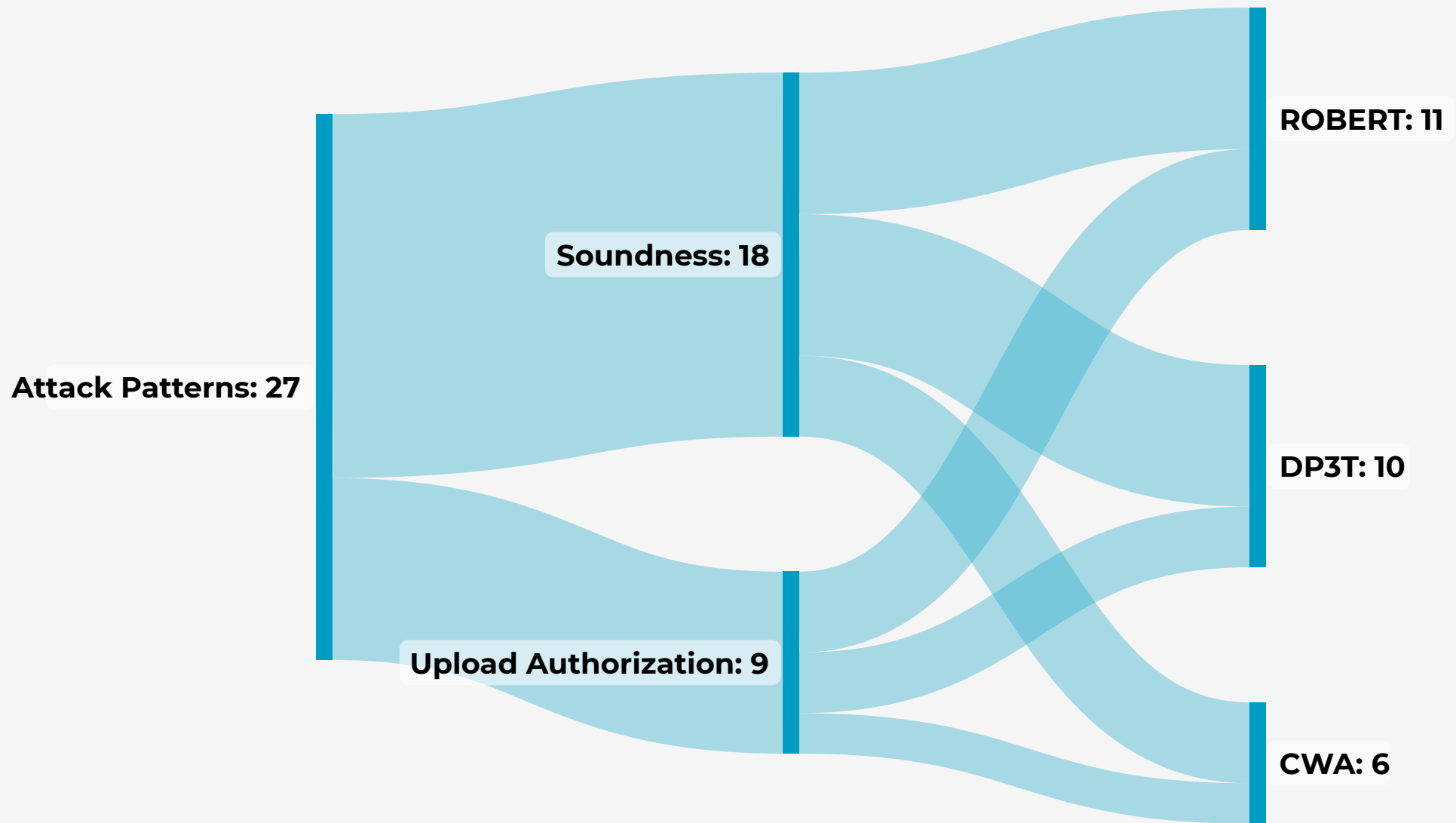
- A priori: **Attacker can do everything!**
- How **does** the attacker **actually** behave?

Soundness
or
Attacker **does** P_1
or **does** P_2
or **does** ...
or **does** P_n





Attack Patterns



Maximum Impact

=





Causing Fake Risk Notifications

Attack Vector		ROBERT	DP3T	CWA
Back end	All-out	All phones	All phones in proximity to some other phone	
	Targeted	Any phone	All contacts of targeted phones	
Health authority	Active	Any phone	All contacts of targeted phone	
	Passive	All contacts of arbitrary phone	Phone-and-test-specific authentication codes	
Infected phones	Modified phone	Contacts of the whole group	Contacts of phone	Max. contacts among group members
	+ Passive antenna	All phones in reach		
	+ Active antenna	Contacts of the whole group	All phones in reach	

Attacker: Group of individuals trying to disrupt the system



Conclusion

- Formal model of **ROBERT**, **DP3T**, and the **CWA**
 - Complex **temporal** and **spatial** interactions between agents
 - Fine-grained **attack patterns** allowing **quantitative reasoning**
 - **27 attack patterns** in total
 - Pushing the practical limit of existing tooling
- **Systematic categorization** of existing and new attacks
 - Understanding of consequences and requirements
- **Possibility of low-risk attack by knowledgeable attacker**

Thank you! Questions?

✉ kevin.morio@cispa.de



GitHub