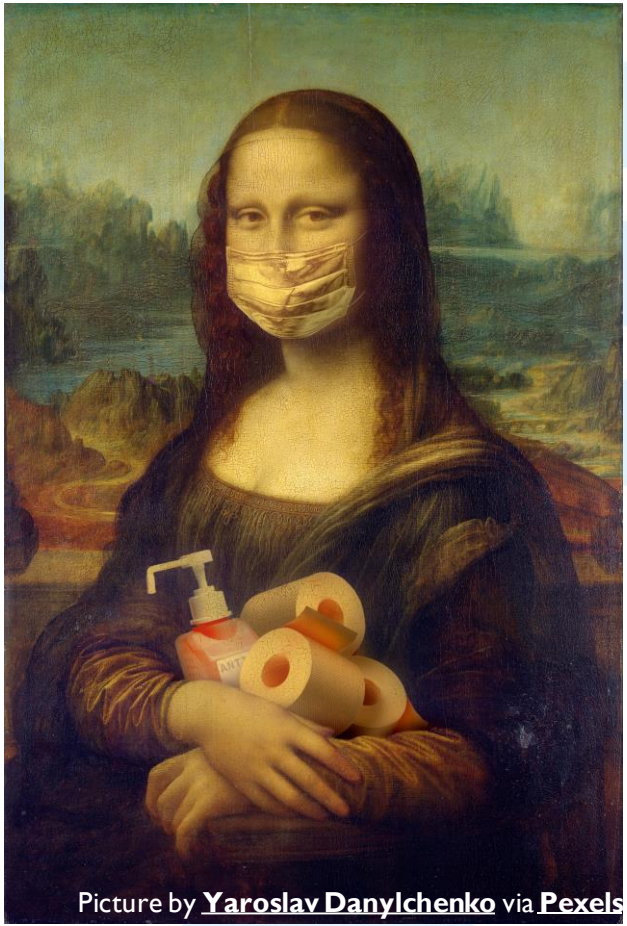
Supporting contact tracing by privacy-friendly registration at catering facilities

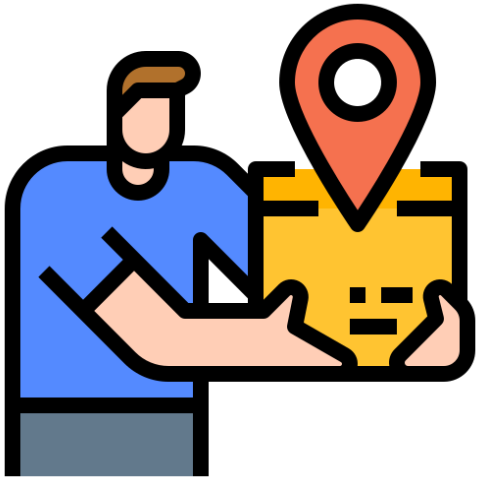
Michiel Willocx

5/9/2020



DistriNet

Limiting the exposure of the population to the virus

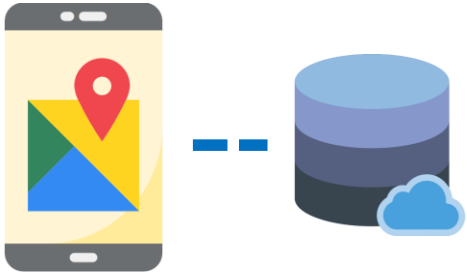
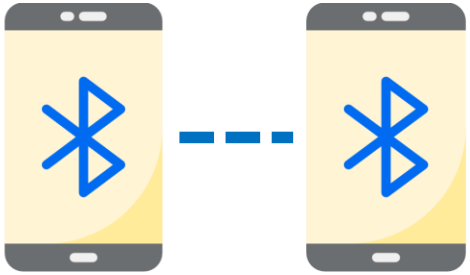


Contact tracing

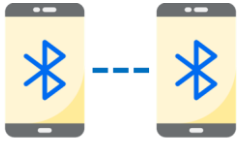
Mandatory registration

Contact tracing

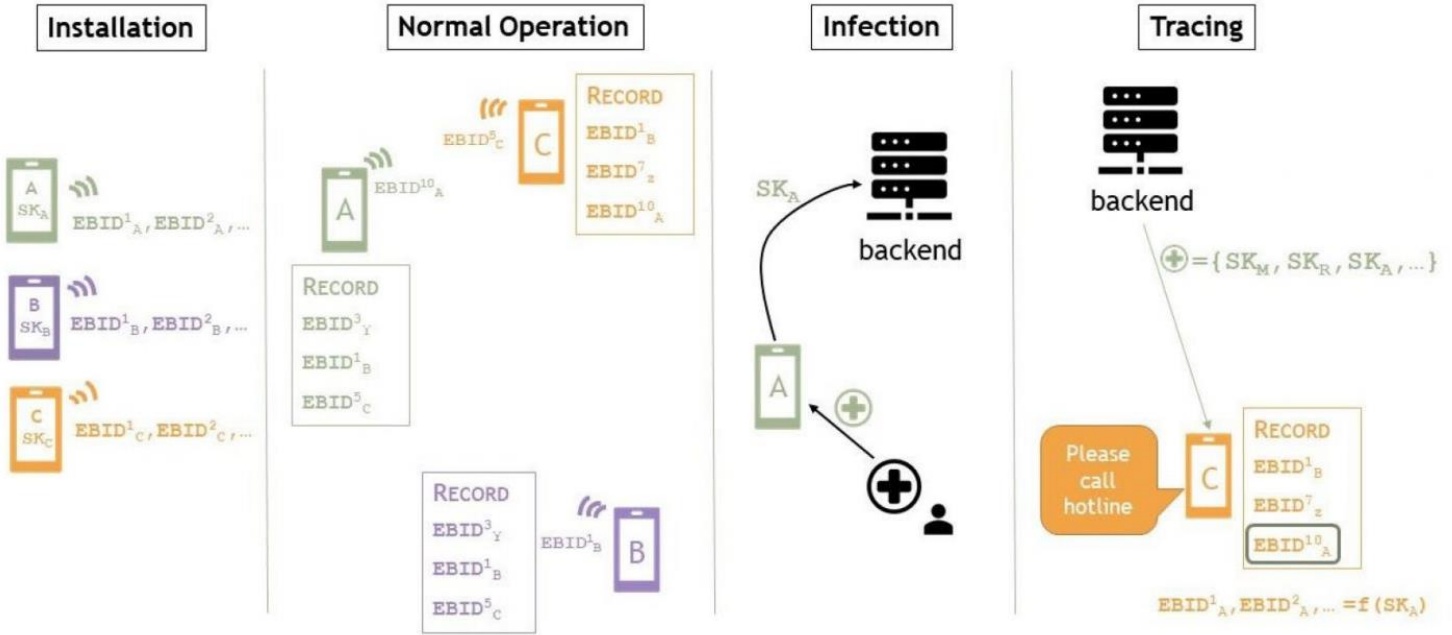
Contact tracing solutions

	 **GPS-based solutions**	Other Solutions With characteristics of both approaches	 **Bluetooth-based solutions**
Where?	China, South korea		Many European countries
Data privacy	☹ ☹		☺ ☺
Data location	Centralized		Decentralized, locally on device
Focus	Track and control infected and non-infected citizens		Inform potentially infected citizens

Example Bluetooth-based solutions



DP-3T

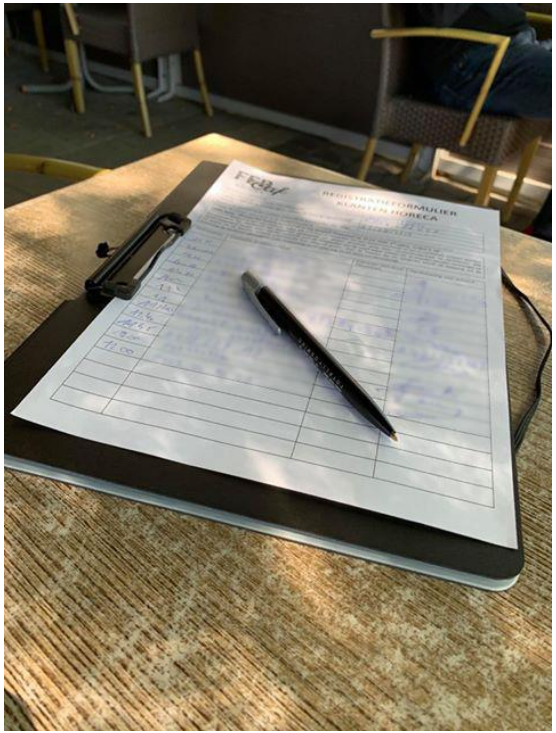


More info: https://github.com/DP-3T/documents

Mandatory registration

Mandatory registration solutions

1. Pen and paper



DistriNet

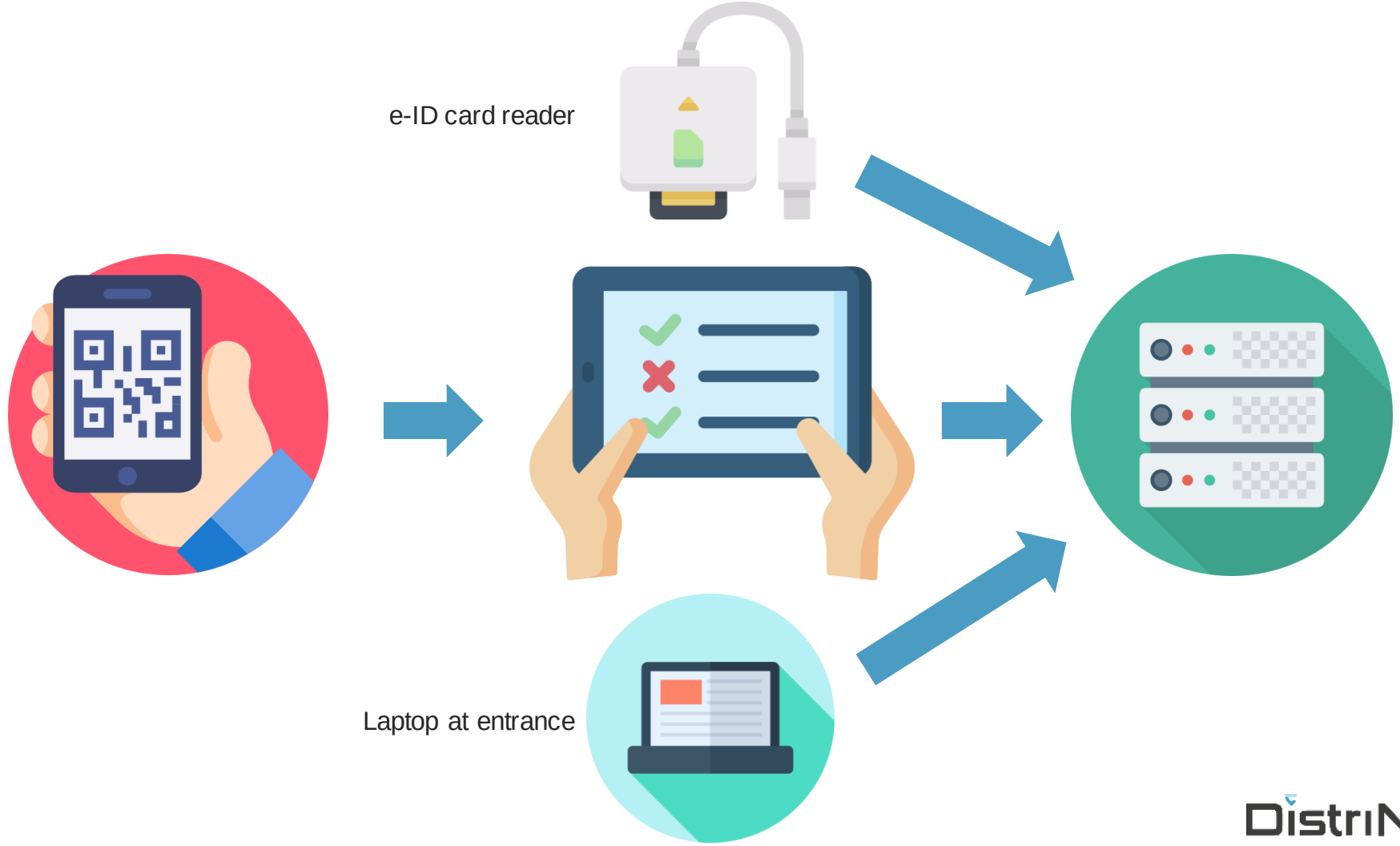
Mandatory registration solutions

2. Naive digital solutions

Visitor scan QR code
→ Redirected to website

Visitor completes questionaire
(name, phone number,…)

Information is stored in the database of a web developer


e-ID card reader
Laptop at entrance

Mandatory registration solutions

3. Our proposal

Requirements

Proximity tracing vs Mandatory registration

Proximity tracing	Mandatory registration
Opt-in, citizens choose to use it	Obligation when entering a catering facility
Active anywhere, anytime	Only applicable in public places
Works location-independent	Location is important information
Users always remain completely anonymous	Must be able to identify and contact users

It is not possible to replace mandatory registration with proximity tracing solutions such as DP-3T, as it supports no location data and has no system in place to identify citizens when required by law.

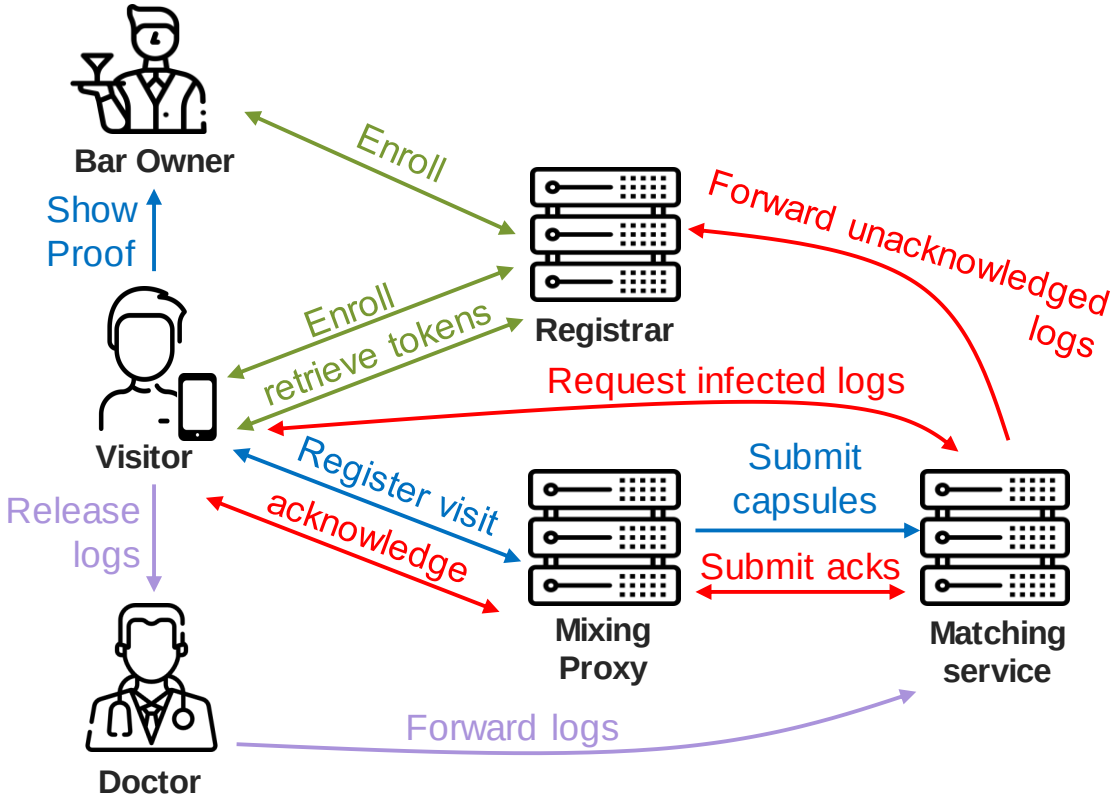
Requirements

Proximity tracing vs Mandatory registration

Proximity tracing	Mandatory registration
Opt-in, citizens choose to use it	Obligation when entering a catering facility
Active anywhere, anytime	Only applicable in public places
Works location-independent	Location is important information
Users always remain completely anonymous	Must be able to identify and contact users

It is not possible to replace mandatory registration with proximity tracing solutions such as DP-3T, as it supports no location data and has no system in place to identify citizens when required by law.

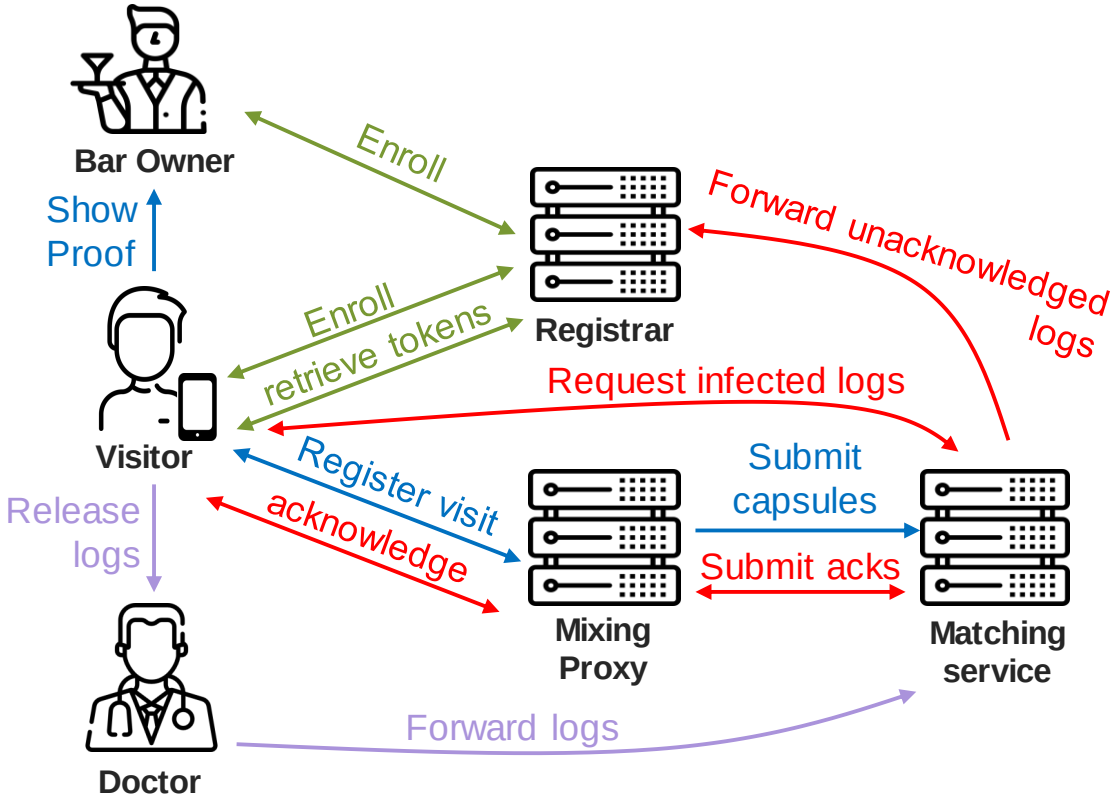
Privacy friendly mandatory registration



- Enrollment
- Visiting a catering facility
- Infection registration
- Informing infected visitors

DistriNet

Privacy friendly mandatory registration



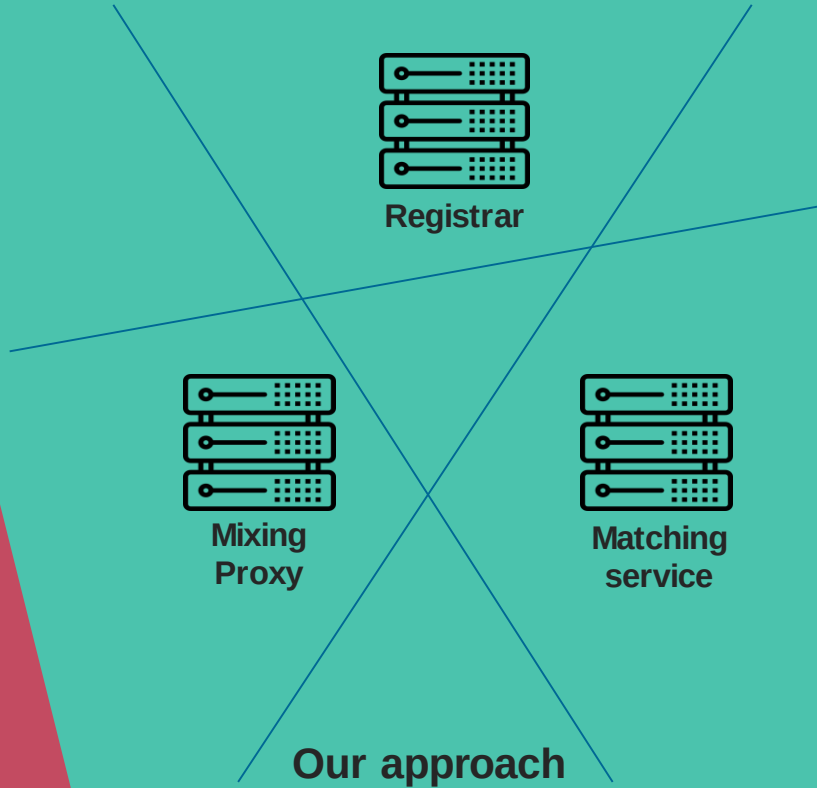
- Enrollment
- Visiting a catering facility
- Infection registration
- Informing infected visitors

DistriNet

Centralized vs Distributed

Name	Phone	Pub	When
Batman	0945 34 25 45	DC lounge	<date> <time>
Iron man	0946 45 76 21	Bar Marvel	<date> <time>
Aquaman	0567 24 98 21	DC lounge	<date> <time>
Ant man	0946 23 56 28	Bar Marvel	<date> <time>
Barry Allen	0867 34 97 54	DC lounge	<date> <time>
Thanos	1094 28 23 45	Bar Marvel	<date> <time>
Superman	7563 23 45 21	DC lounge	<date> <time>

Current SOTA



Our approach

Linkability

T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$ ⬅

T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$ ⬅

T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$

T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$

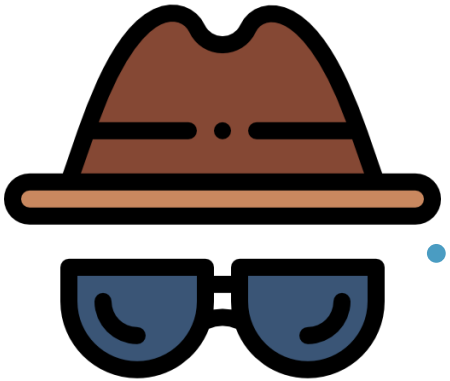
T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$

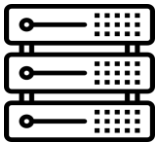
T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$ ⬅

T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$

T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$ ⬅

T^{user}_{x,day_i} $H(R_i, nym_{CF,day_i})$





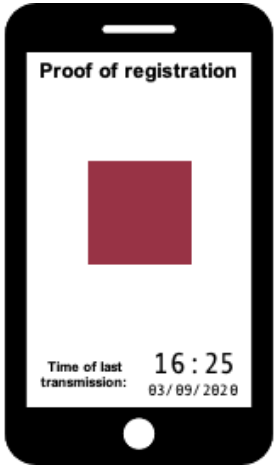
Matching service

There is currently
"*4 people*" in "*a bar*"

DistriNet

Users can tamper with the system

- Bypass the system
  - Visitors can try to avoid to use the system



- User can not provide correct proof without scanning and registering
  - Signature by mixing proxy
- Bartender checks proof before ordering

Users can tamper with the system

- Flooding
  - Fill database of matching server with nonsense
  - !! On infection – huge increase in download size for users !!

Prevention:

- Limited amount of tokens T_{x,day_i}^{user} for each user
- New, unused token is required for new entry in database

Users can tamper with the system

- Fake infections
  - Introduce false infections in the system

Doctor

Prevention:

Only capsules that are signed by the general practitioner will be accepted by the matching server.

Visitor

Conclusion

- Privacy-friendly alternative for mandatory registration in bars and restaurants

- Potential to apply the same strategy for other problems in other domains.
  - E.g. Animal transport

Thank you!

michiel.willocx@kuleuven.be