

# The Cluster Exposure Verification (CLÉA) Protocol

<https://github.com/TousAntiCovid/CLEA-exposure-verification>

**V. Roca, A. Boutet, C. Castelluccia (Inria, PRIVATICS team, FR)**

May 10<sup>th</sup>, 2021



# Goals



- focus on **public/commercial locations** (restaurant, bar, sport center, show, train, shared ride) and **private events** (wedding, private party)
- **easy “check-in”** to a location, by scanning a QR code, on site or in advance, or filling a hand-written register, according to user preference
- automatically **detect** potential cluster locations/events
- automatically **notify** a user who shared, at the same time, a location/event with one or more COVID+ users



## Two key design choices:

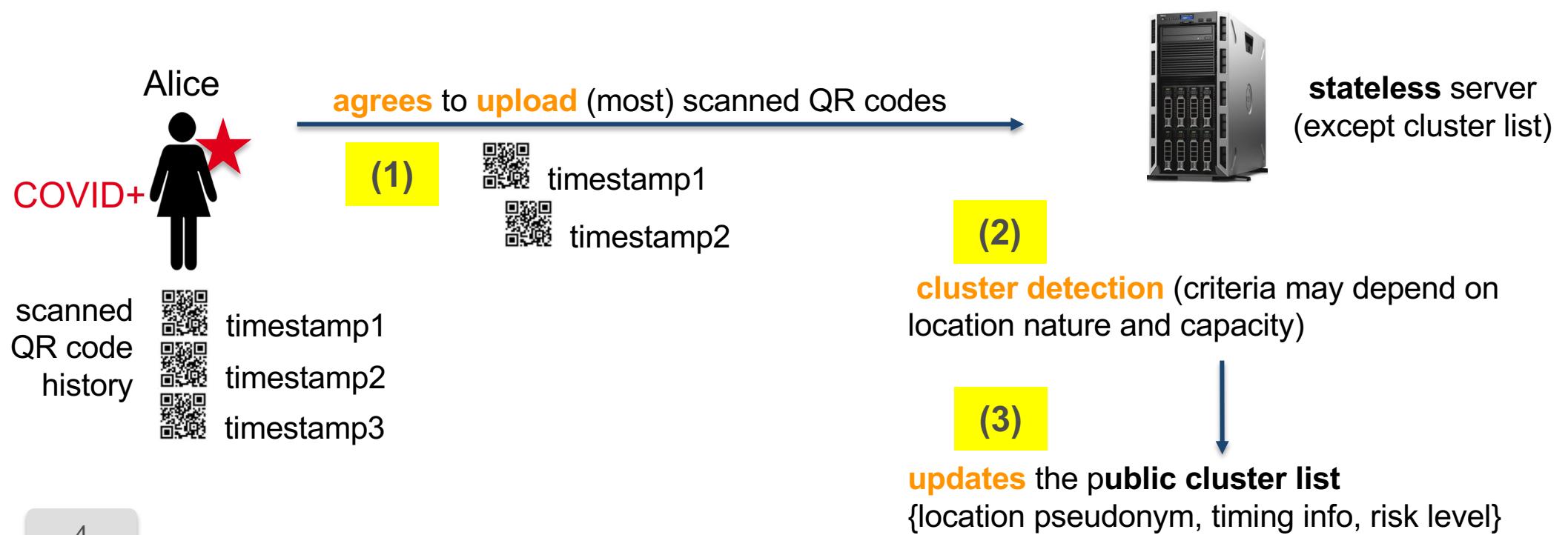
#1: centralized cluster detection

#2: decentralized risk estimation and notification

and a direct consequence, a **public list** of cluster pseudonyms

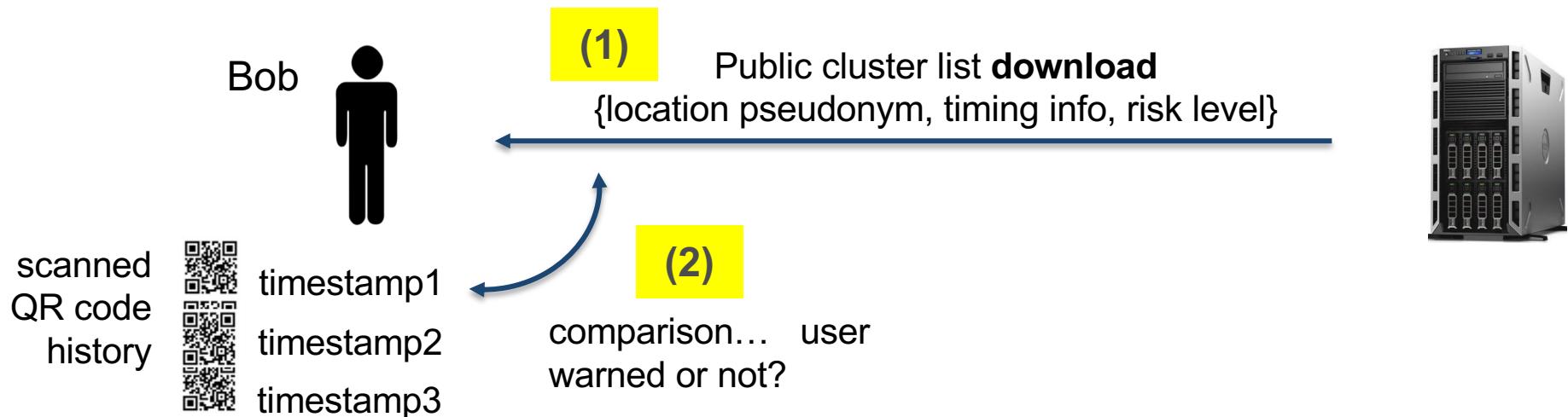
# Key choice #1: centralized cluster detection

- COVID+ users are invited to upload their scanned QR codes + timing
- server detects clusters and updates {location pseudonym, timestamp + duration} cluster list



## Key choice #2: decentralized risk estimation/notif.

- scanned QR codes remain on the user smartphone (if not tested COVID+)
- compares scanned QR codes with the cluster list info



## Key choice #2: decentralized risk estimation/notif. (2)

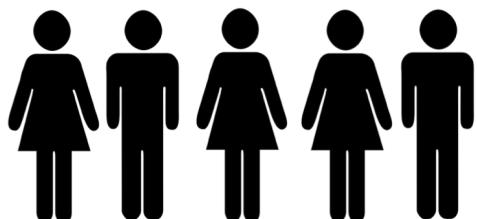
- decentralized risk analysis requires sharing cluster list: {loc. pseudos; timing info; risk level}
  - this is **not** sensitive medical data per se
  - with dynamic QR codes, pseudonyms are temporary 😊

situation totally different from **contact tracing** where decentralized risk analysis (e.g., GAEN) requires to share publicly the pseudonyms of users tested COVID+

- it's **sensitive health** data 😢, and anyone can easily know if a neighbor is COVID+
  - see: <https://coronadetective.eu>
  - GAEN is not very GDPR friendly

## A **single** protocol, CLÉA, **three** potential deployments

Key question: which role for the Manual Contact Tracing Team?

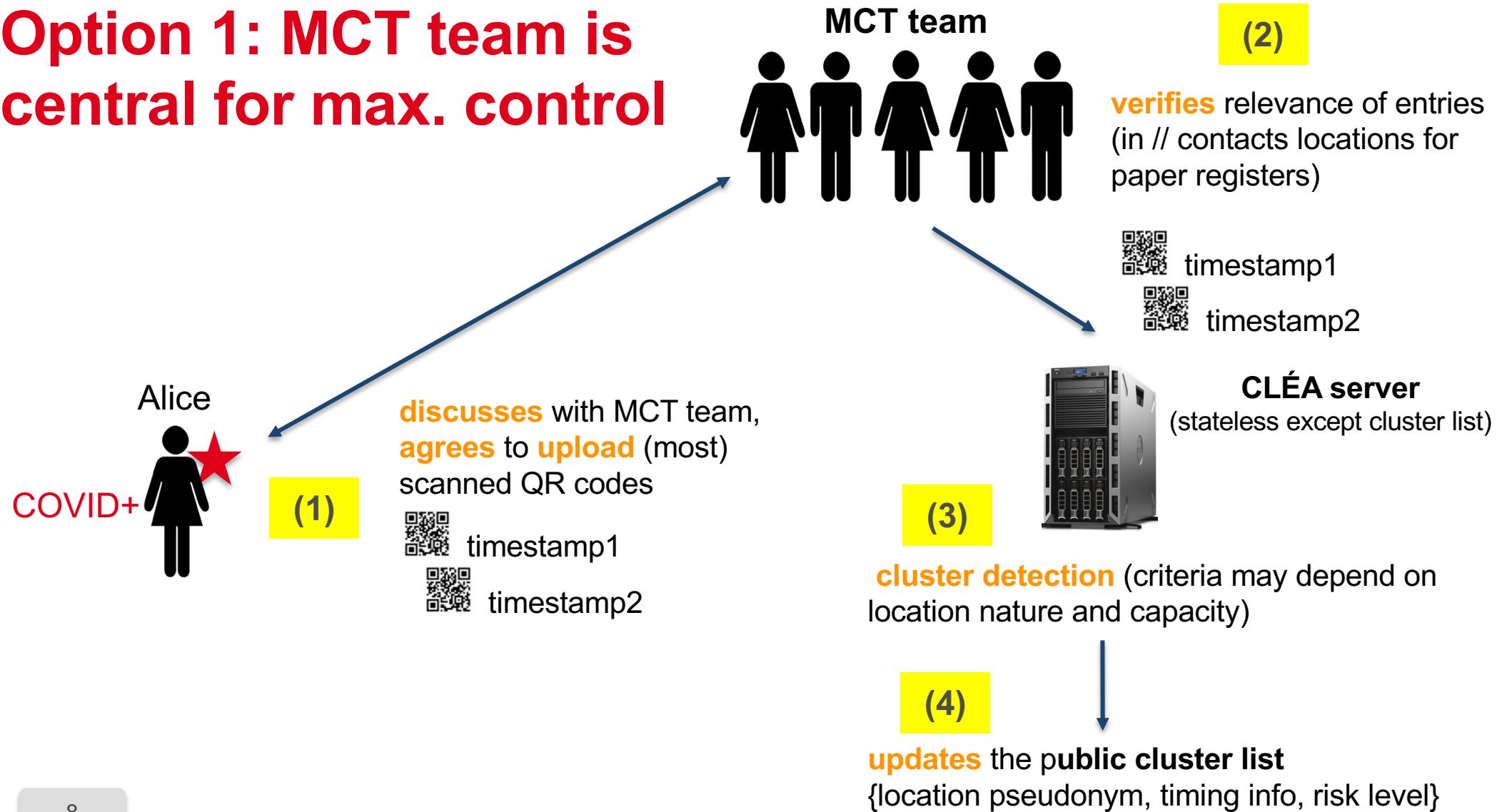


**option1:** the MCT team is at the center for maximum control

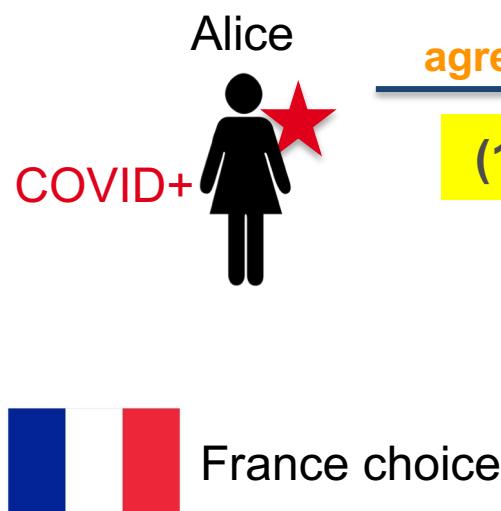
**option2:** do not overload the MCT team for maximum scalability and speed

**option3:** no MCT team involvement

# Option 1: MCT team is central for max. control



## Option 2: do not overload the MCT team for max. scalability and speed



agrees to upload (most) scanned QR codes

(1)



timestamp1

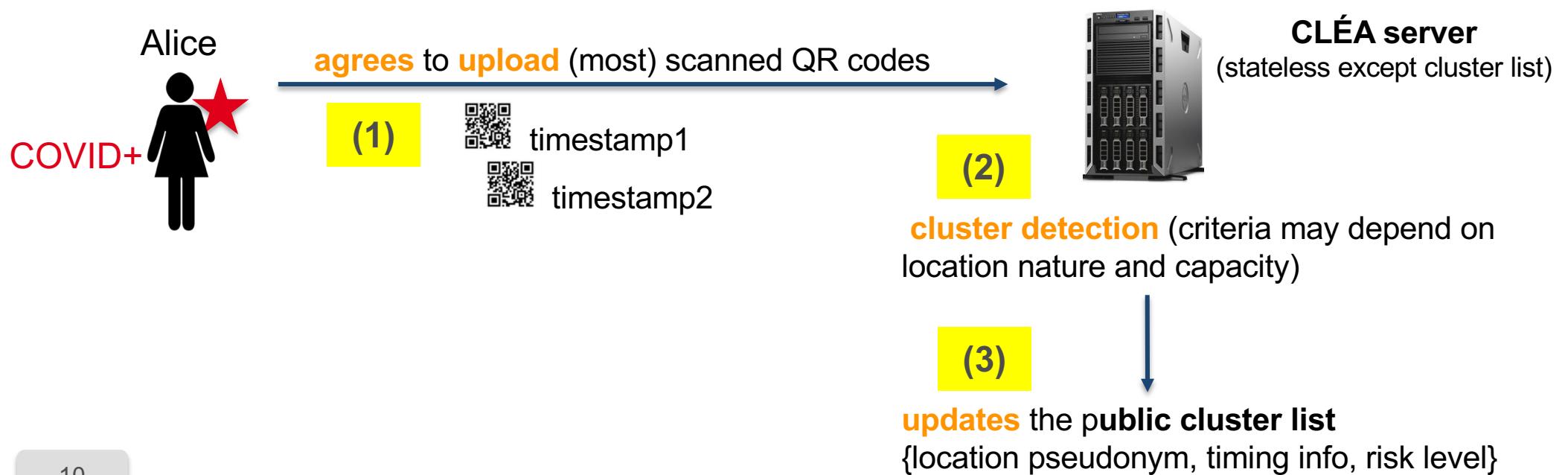


timestamp2



# Option 3: no MCT team involvement

- QR codes no longer contain any MCT team information, processing purely automatic



## **Additional technical considerations:**

- structure of a QR code
- static or dynamic QR code?
- compatible with dedicated plug-and-play devices
- QR codes for synchronous versus asynchronous scans

# Structure of a QR code

- a 65x65 (level 12, M or Q redundancy, binary) QR code



- contains a “deep-link” URL

- example (FR):

<https://tac.gouv.fr?v=0#O9QAalpq3qpQP...N2qpcAA0dmaCQ>

**country** specific prefix

**location** specific dynamic suffix  
(after Base64url encoding)

- a scanned QR code

- is either automatically managed by the CLÉA application (if installed)
  - otherwise user is redirected to the <https://tac.gouv.fr> web site

## Structure of a QR code (2)

- location specific suffix
  - **cleartext part:** essentially the location pseudonym (Location Temporary ID)
  - **encrypted part:** essentially the location key, plus location typology, and encrypted location contact information

```
LSP(t_periodStart, t_qrStart) = [ version | LSPType = 0 | reserved1 | LTId(t_periodStart)
| Enc(PK_SA, msg) ]
```

cleartext (incl. location pseudo)

where:

```
msg = [ staff | locContactMsgPresent | reserved2 | CRIexp | venueType | venueCategory1 |
        | venueCategory2 | periodDuration | ct_periodStart | t_qrStart | LTKey(t_periodStart)
        | Enc(PK_MCTA, locContactMsg) if locContactMsgPresent==1 ]
```

# Static or dynamic QR code?

- **issue:** we have a **public** cluster list {cluster location pseudonyms + timing info}
- **dynamic QR codes:**
  - **mitigates** trivial cluster cartography attacks, since pseudonyms change all the time
  - **mitigates** replay attacks since QR codes have a limited time validity
  - **improves user privacy**, since two users at the same location across two different days cannot be linked (they upload different pseudonyms if COVID+ and their phones, if seized, contain different pseudonyms)
- try to be **as secure as possible**, although no full-proof guaranties

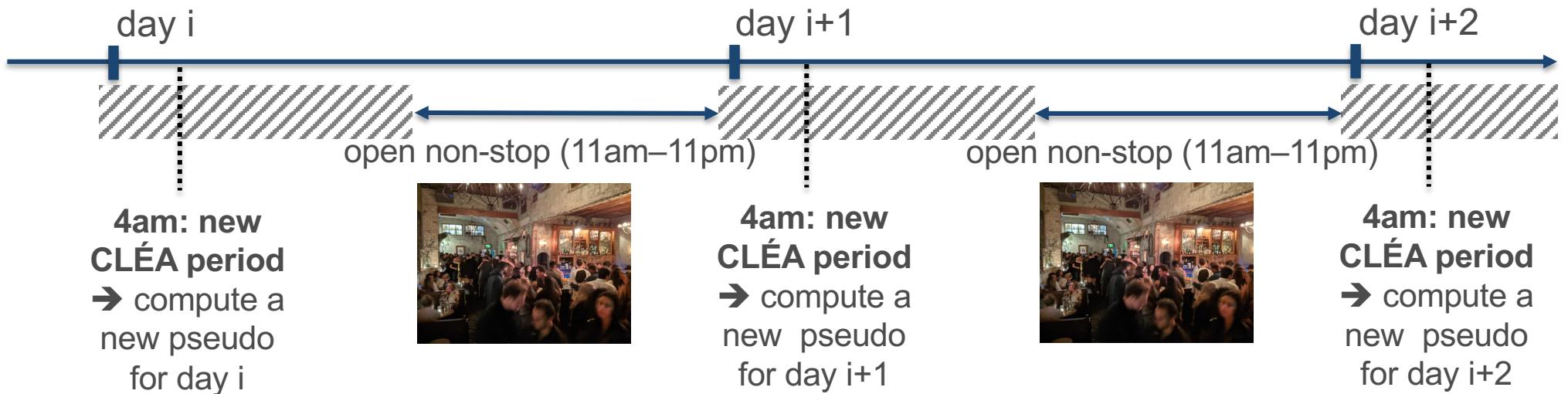


Mitigate trivial cluster cartography attack



## Static or dynamic QR code? (2)

- example: compute a location temporary pseudonym (LTId) per day



```
LTKey(t_periodStart) = SHA256(SK_L | t_periodStart)  
LTId(t_periodStart) = HMAC-SHA-256-128(LTKey(t_periodStart), "1")
```

# Compatible with dedicated plug-and-play devices

- an **easy to deploy** solution for public/commercial locations and **dynamic** QR codes
  - an option, not an obligation
- pre-configured, install-and-forget **commercial devices** (e-ink 200\*200pix. display)
  - no onsite configuration, comes ready to use
  - no wireless connection / power plug / USB connector / button
- **one or more devices** per location, depending on size
  - all devices compute the same location pseudonym

static, printed  
QR code



OR



dynamic QR  
code

<https://www.skiply.eu/ubiqod-key/>

# Synchronous vs. asynchronous scans

enter a location, scan the QR code



receive a QR code (e.g., on your plane ticket), scan it, and later on, take your plane

OR ?



## Synchronous vs. asynchronous scans (2)

- CLÉA addresses both models
- two QR code types that differ WRT to timing information
  - **synchronous scan:** presence starts with scanning time (dynamically known)
  - **asynchronous scan:** presence starts with the timestamp included in the QR code (scanning time is meaningless). QR code is necessarily static. Relay attacks are potentially easy if the QR code is widely distributed...

## **Important particular cases:**

- 1.** employees
- 2.** private events
- 3.** linking CLÉA and hand-written attendance register
- 4.** pan-European interoperability

# Particular case #1: the location employees

- employees must benefit from CLÉA (be warned if the work place is cluster)
  - major difference: an employee stays in the location for longer periods than a client
  - since scanning every 2 hours is not a solution, a device can produce a “Staff” QR code
    - a “Staff” QR code is valid till the end of current period
    - (NB: a magnetic detector on a Skiply device enables to produce a “Staff” QR code)
  - the employee CLÉA app recognizes the “Staff” QR code and its extended duration to assess risks
- an employee tested COVID+ should be able to upload her scanned QR code history
  - the CLÉA server recognizes the “Staff” QR code and its extended duration to assess risks
- easy to address ☺

## Particular case #2: private events

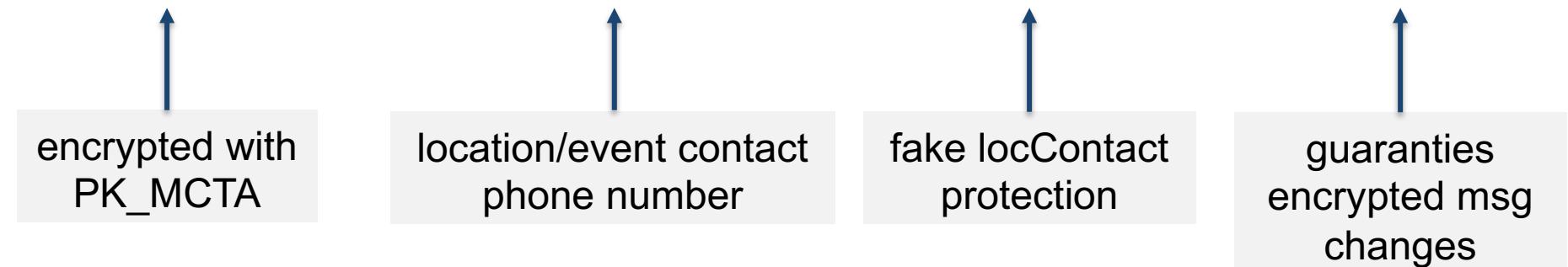
- choose a **static, printed QR code**
  - to be generated on a Web service, printed and displayed at the entrance
  - it's necessarily a static, time limited (for this event) QR code
  - event may last more than a single day...
  - it's possible to generate/send a QR code for asynchronous scans

The same CLÉA system handles both static and dynamic QR codes the same way  
(no protocol change)

## Case #3: Linking CLÉA and hand-written registry

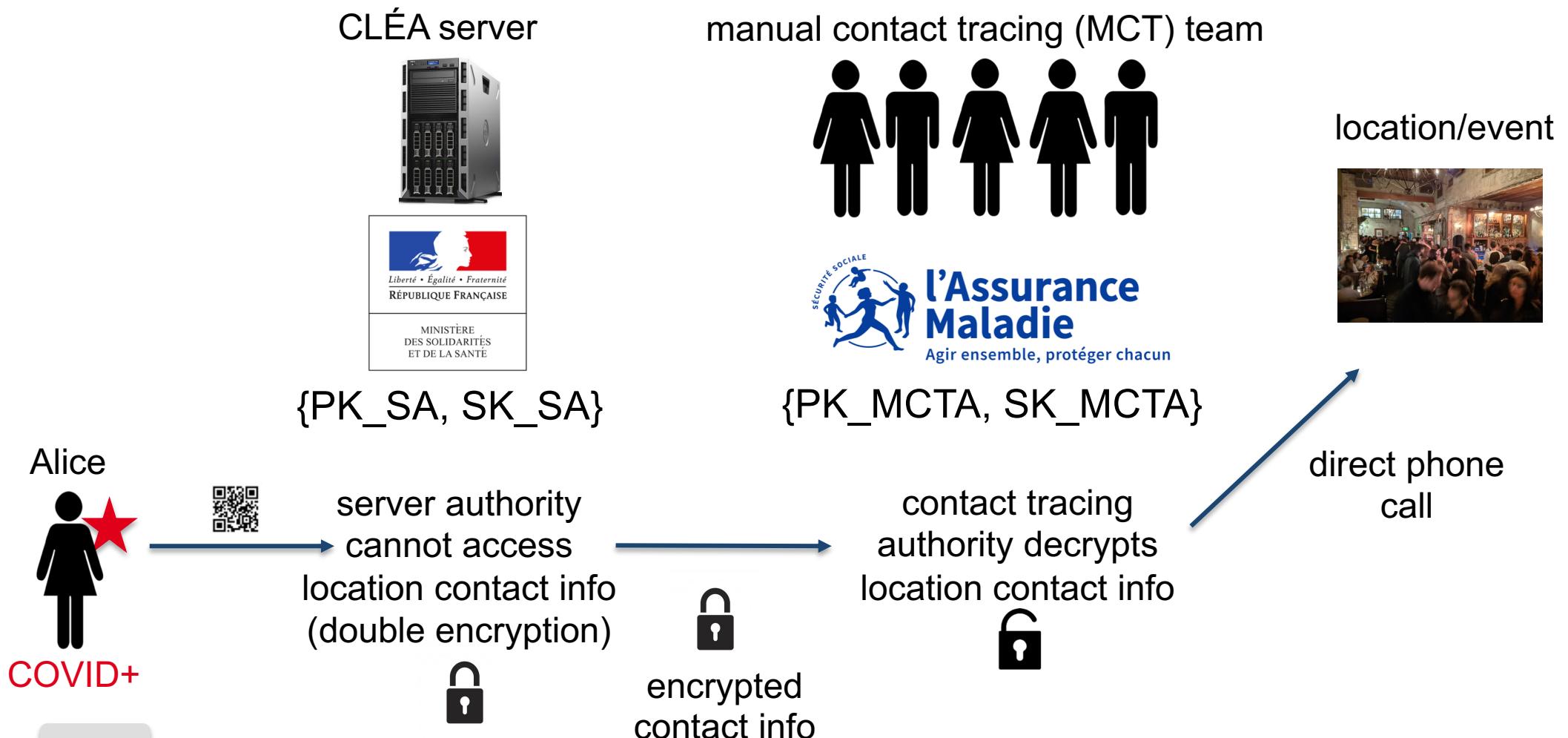
- CASE 1: a user tested COVID+ has used the CLÉA system
  - a link is necessary to inform the location/event manager, get the registry, inform others
  - QR code contains encrypted contact information

```
locContactMsg = [ locationPhone | locationPIN | t_periodStart ]
```



- only the Contact Tracing Team Authority can decrypt it (it's a different authority)

# Linking CLÉA and hand-written registry (2)

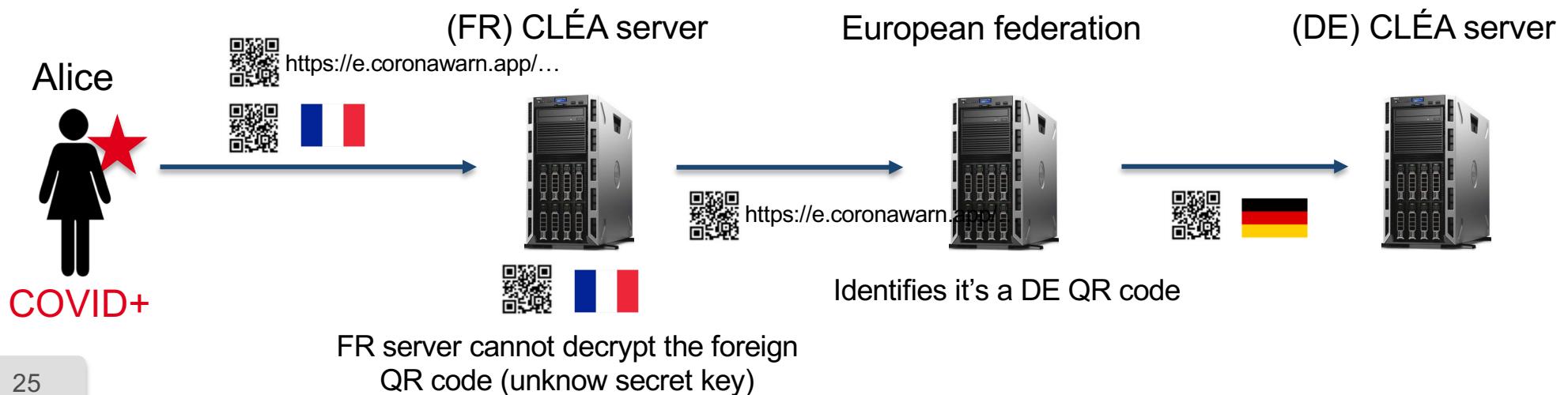


# Linking CLÉA and hand-written registry (3)

- CASE 2: a user tested COVID+ has used the hand-written registry
  - *assumption 1: the user remembers having been to a location and when*
  - the MCT team asks the location/event contact to send the paper attendance registry...
  - ... and a QR code generated that day
  - *assumption 2: the location contact has scanned a QR code that day*
  - the location contact uploads the QR code, the MCT team identifies the location pseudonym used that day, and can inform the CLÉA server (details TBD)
- involves a few risks, yet seems realistic
  - because the location contact person has a personal interest in scanning QR codes

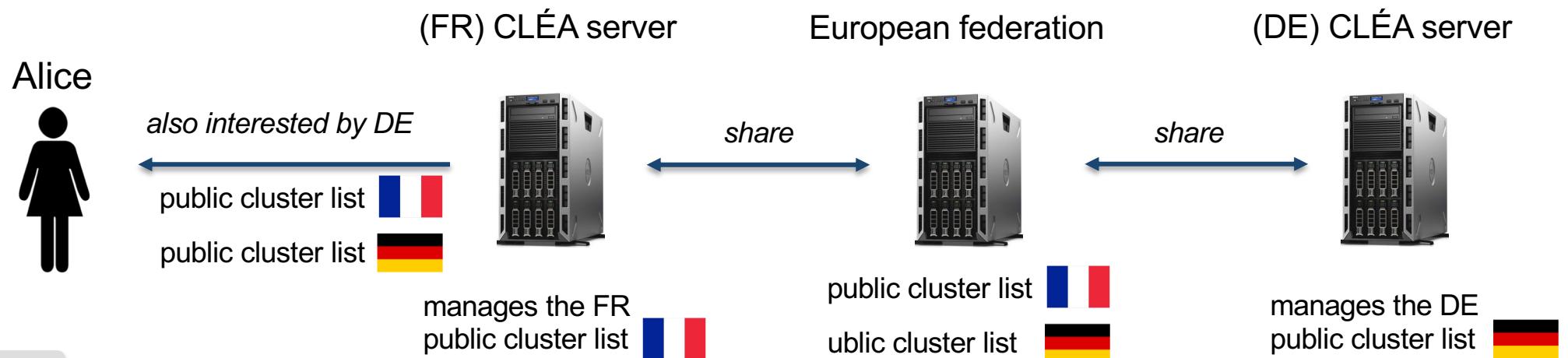
# Particular case #4: pan-European interoperability

- QR codes do include a country specific prefix in the URL
  - includes a FQDN (e.g., [tac.gouv.fr](https://tac.gouv.fr) for France) that indicates country of origin
- Example: Alice, who went to a German restaurant, is tested COVID+ and agrees to share her scanned QR codes...



## Particular case #4: pan-European interoperability (2)

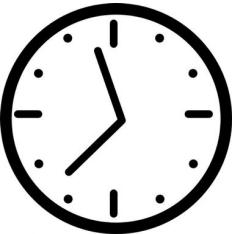
- National servers also need to share their public cluster list
- Example: Alice, who went to a German restaurant, wants to know if she is at risk...



# Summary

# CLÉA benefits

- **Speed-up** notifications because “**time is key**”
  - each scanned QR code is immediately usable by the CLÉA server  
(because scanned QR codes are self-sufficient ☺)
- **Minimize MCT team work** in the critical path (even with option 1)
  - cluster qualification/user notification is automatic
  - no need to search a phone number and contact the location/event manager  
(because scanned QR codes are self-sufficient ☺)

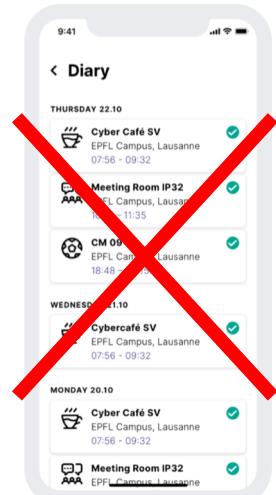


# CLÉA benefits (2)

- Minimize practical risks for **maximum reliability**
  - users no risk to “forget” inadvertently visited locations  
(because scanned QR codes are self-sufficient ☺)

?

- Preserve **user privacy** as much as possible
  - manipulate, store, send location (rotating) **pseudonyms only**
  - never store real location names and addresses!  
(because scanned QR codes are self-sufficient ☺)



# CLÉA benefits (3)

- **Reduce risks of attacks** by asking a “proof of presence” in a location
  - although not perfect, a location cannot be qualified cluster unless a valid scanned QR code is exhibited
- Enable efficient **interoperability** across borders
  - a Country Code for efficient routing of QR codes
  - accommodates different national deployment choices



- fast, practical, flexible, interoperable, natively designed for presence tracing and cluster detection
- added in **April** to the French TousAntiCovid app
  - *NB: added does not mean used (re-opening in June...)*
  - CNIL and ANSSI reviews under progress
- documents and open-source code
  - <https://gitlab.inria.fr/stopcovid19/CLEA-exposure-verification>
  - <https://github.com/TousAntiCovid/CLEA-exposure-verification> (github mirror)



Thank you...

Contact: [vincent.roca@inria.fr](mailto:vincent.roca@inria.fr)