

ACE* - Analytics on Covid Exposure Networks

Crypto hackathon 2021

Alen Orbanić, Jan Grošelj, Boris Horvat

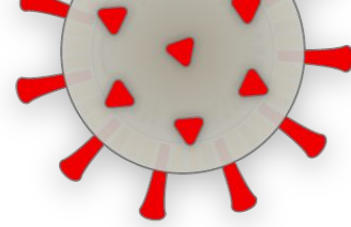


ACE* project in a glance

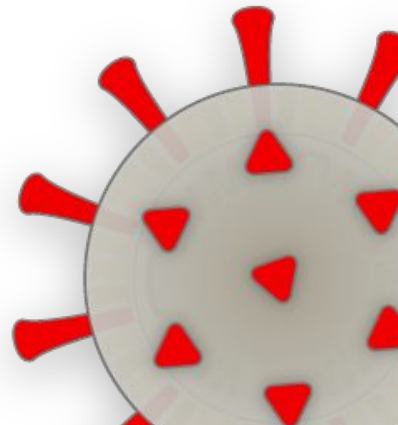
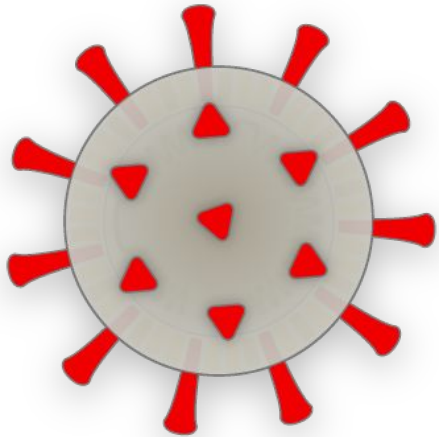
WHY? The objective of this project is to **get insights about the actual social distancing** during Covid-19 epidemic, directly from the participants.

HOW? Our plan is to **leverage the data of actual exposure networks**, gathered by multiple Corona-Warn-App (CWA) apps, and their analysis, **using decentralized multi- client functional encryption for inner product FE scheme**, while at all steps respecting data privacy and safety, by processing a minimum of required personal data that is handled with maximum protection.

WHAT? We have implemented proof-of-concept (PoC) implementation of the core infrastructure for trusted submitting, processing, and visualization of Covid-19 exposure networks, together with working simulation.

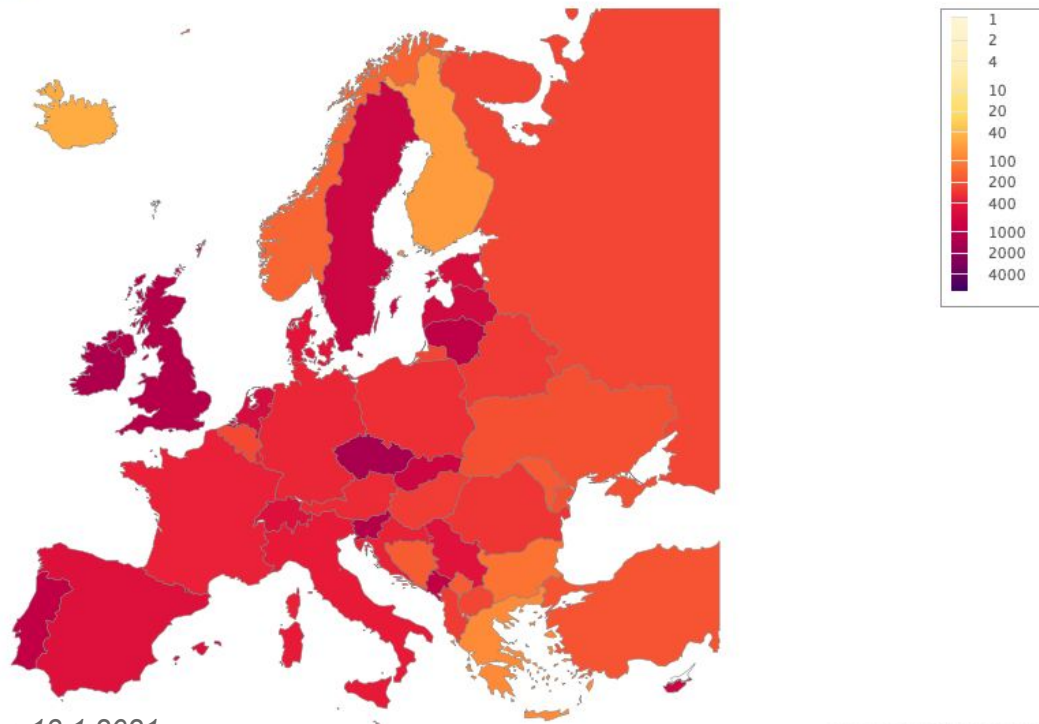


WHY?



COVID-19 :: Situation in Slovenia (EU) can be better

14 days incidence per 100,000 people Weekly increase Restrictions and imported cases



Source: COVID-19 Tracker Slovenia & NIJZ, obtained on 13.1.2021

data source: NIJZ, Our World in Data

Social distancing is the key preventive measure ...*

A person who has been in close contact with another person who tested positive in a coronavirus test, must **limit their contact** with other people.

In public space, consistently **maintain a safe distance** of 2m from other people.

Persons with a confirmed infection **must inform other** close contacts.

All those who have been informed that they have been in close contact with an infected person, **must stay home**.

** ... for restricting the spread of the virus; by Slovenian Health authorities*

Corona-Warn-App (CWA) - unified tracking approach

CWA is an **open source project** (mobile app + servers) that helps trace infection chains of SARS-CoV-2, from Germany.

It uses a decentralized approach, with focus on data privacy and safety, (Privacy-Preserving Contact Tracing specifications by Apple & Google), and **notifies users** if they have been exposed.

CWA is specifically designed to ensure for each step that the app processes a minimum of required personal data that is handled with maximum protection - for the following **2 objectives**:

- assess personal risk of infection,
- learn COVID-19 test results faster.

Source: <https://www.coronawarn.app>



CWA is used for tracing exposure to SARS-CoV-2

- **To assess personal risk of infection**, app
 - automatically collects nearby identifiers (< 2 m or > 15 min),
 - distributes list of keys of SARS-CoV-2 confirmed users,
 - checks for exposure to SARS-CoV-2 confirmed users.
- **To help learning COVID-19 test results faster**, app
 - enables communication (retrieve, inform) of user's test result, after explicit consent from the user.



#OstaniZdrav (#StayHealthy) = CWA in Slovenia

The #OstaniZdrav application is **a CWA app clone** (maintained by Slovenian Health Authorities) that

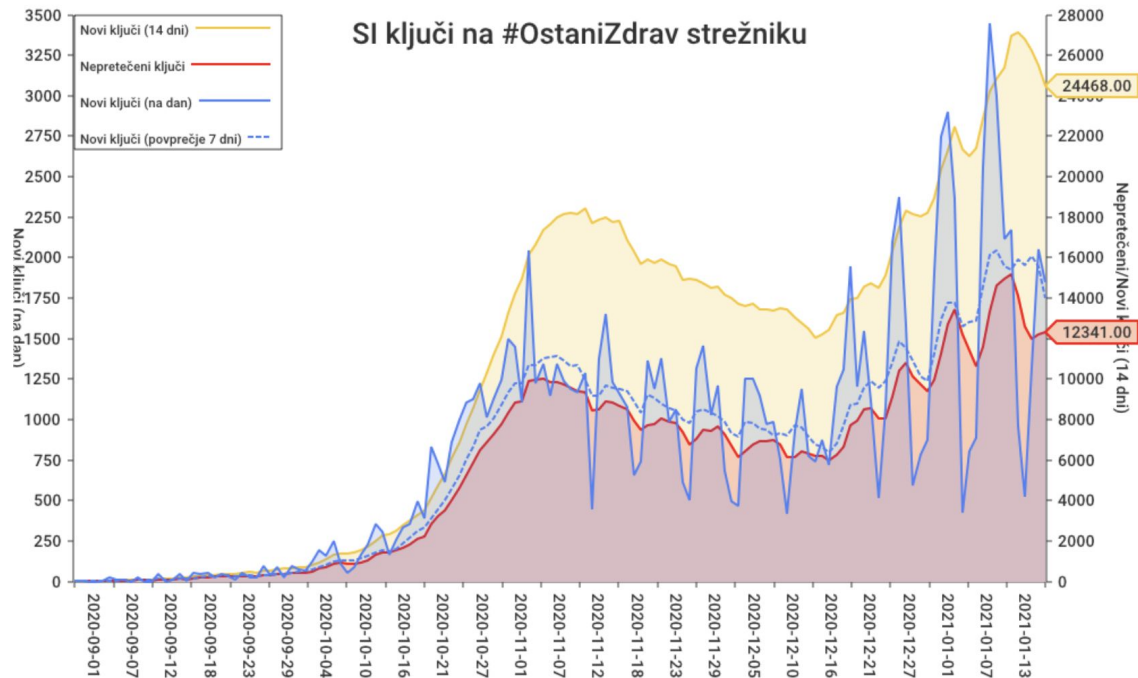
- informs the user about contact with an infected person,
- enables user to enter TAN code received from the epidemiologist.

Goal: To help contain and manage the spread of infection and reduce the burden on the healthcare system, thus **enabling the state to control** the virus, by using less coercive measures.

!!! But !!!, the Health Authorities do not have any information about the app usage, virus spread, social distancing, nor control.



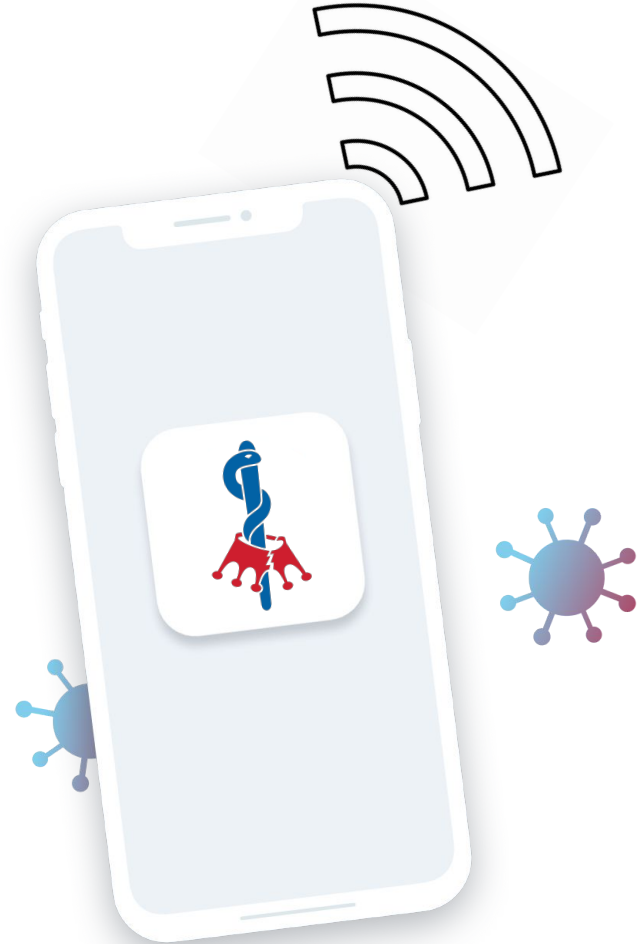
#OstaniZdrav (#StayHealthy) = CWA in Slovenia



OUR OBJECTIVE

To get insights about the
actual social distancing
from the field ...*

* ... during COVID-19 epidemic, from the CWA app users, to help Health Authorities manage the spread of infection (by using less coercive measures).

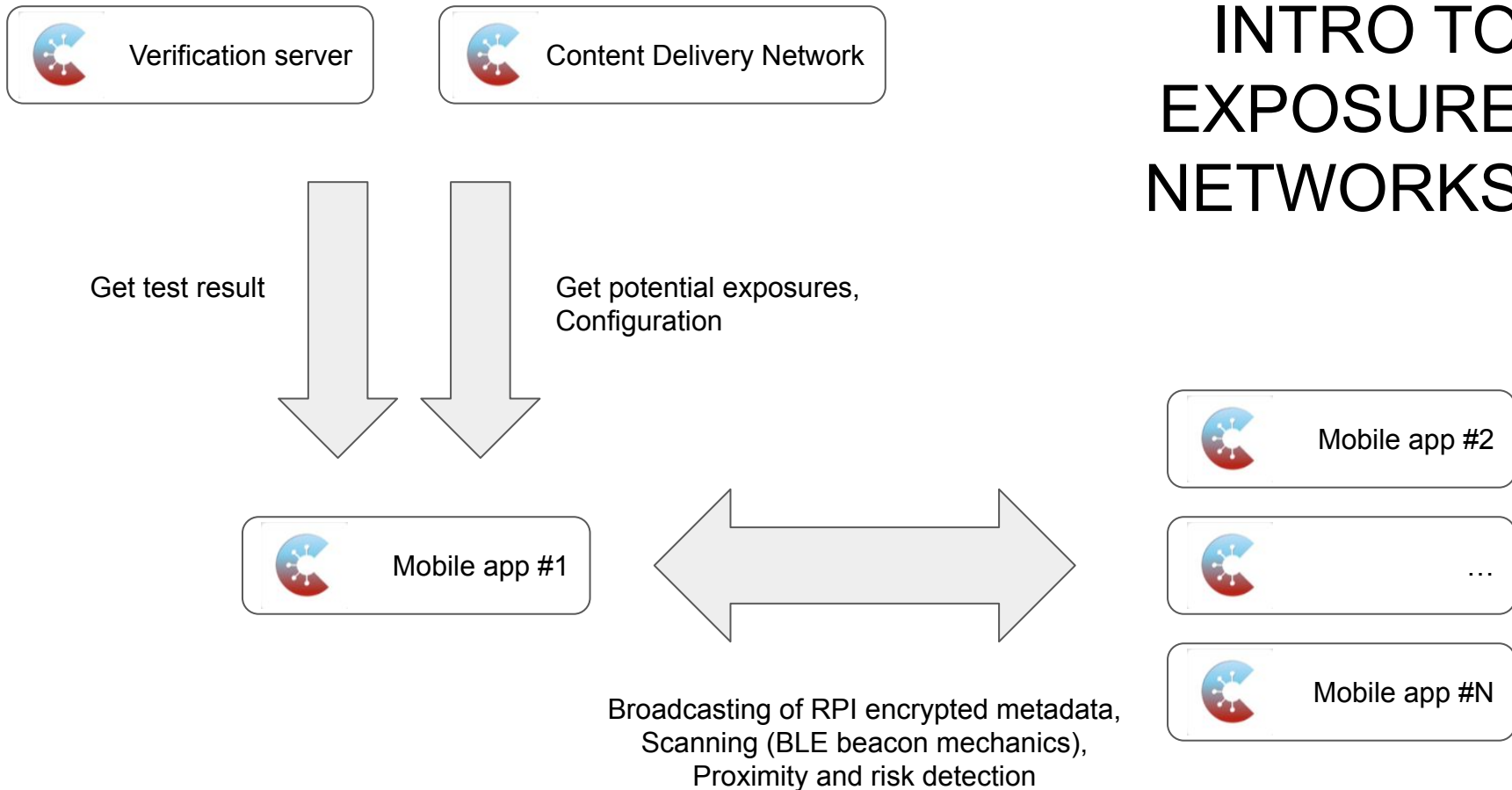




A diagram featuring three virus-like particles (VLPs) arranged in a triangular pattern. Each VLP is a light gray sphere with red triangular spikes on its surface and a ring of red triangles around its equator. They are connected by a dashed line of small gray squares. The word "HOW?" is centered in the middle of the triangle.

HOW?

INTRO TO EXPOSURE NETWORKS



INTRO TO EXPOSURE NETWORKS



Verification server

- **Test results** for verified TAN



Content delivery network

- **Aggregated keys** of positively tested individuals
- **Configuration parameters** for the risk scores

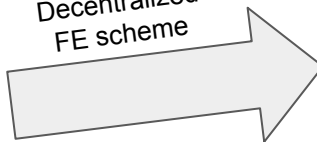
Health authorities can set weights for: Bluetooth attenuations, infectiousness of the affected individual and diagnosis report type, notification thresholds.



Mobile app #1

- **Public exposure data**

Decentralized
FE scheme



Analytics server

- **Meaningful analytics**

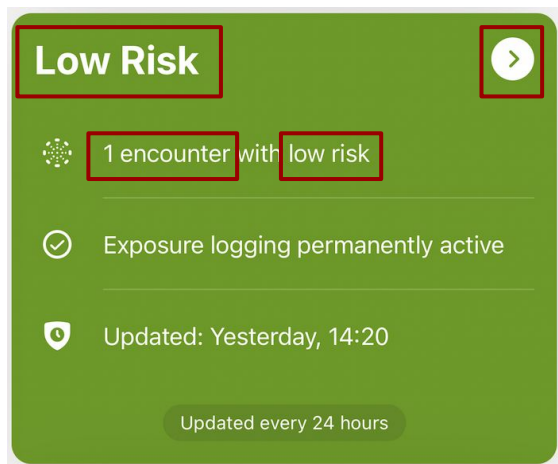
PRIVATE DATA + RESTRICTIONS ON LOCATION DATA AND DATA USAGE

- Own Rolling Proximity Identifiers (**RPI**), changed every ~15 min

Exposure notification framework gives access to **local secure storage** for up to 14 days:

- Collected RPIs of encounters & metadata: day the contact occurred, how long it lasted and the BT signal strength of the contact
- Own Temporary Exposure Keys (TEK), changed daily, own Diagnosis key

ENF provides no access to the exposure network



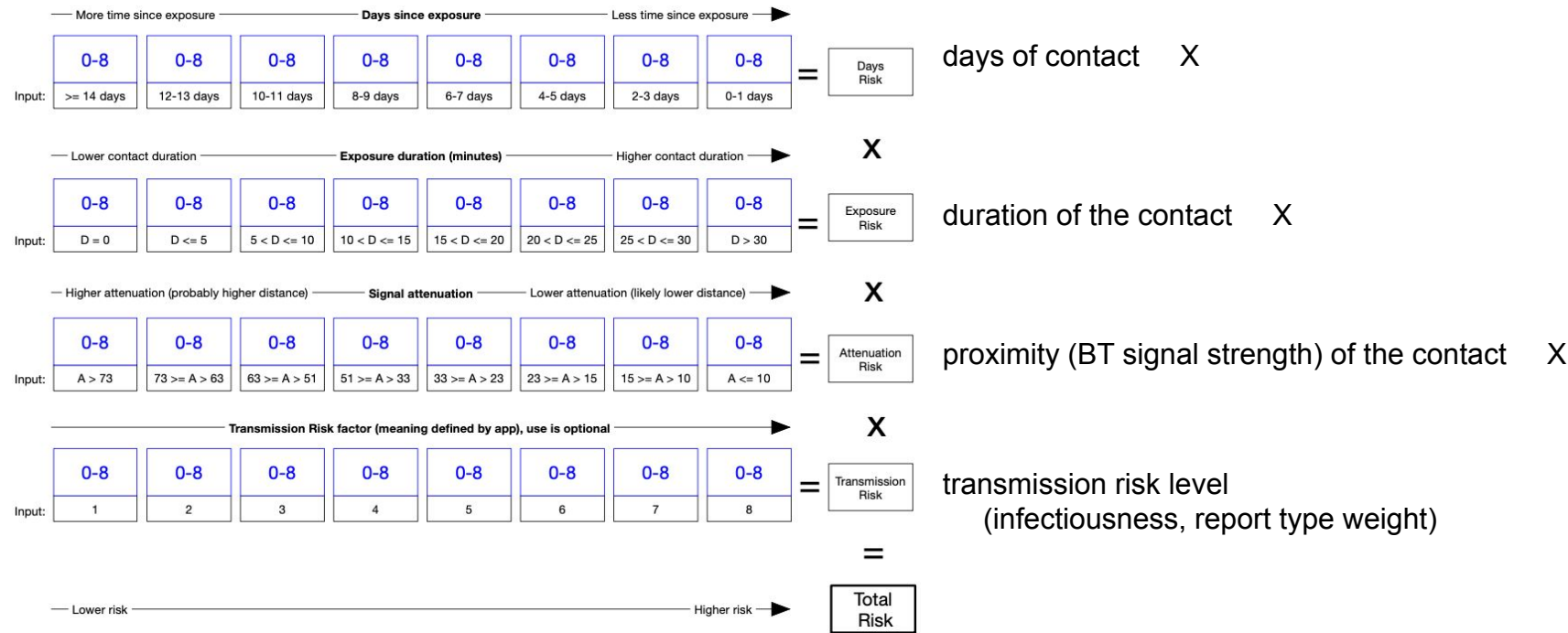
Due to privacy preserving, **nobody (neither the app) has access to the network**, including the local encounters!

Hence, (without the protocol upgrade) we cannot reconstruct the parts of the network.

But, **the data about the user's risk profile and number of identified exposures through the time are available to the mobile app**, specifically:

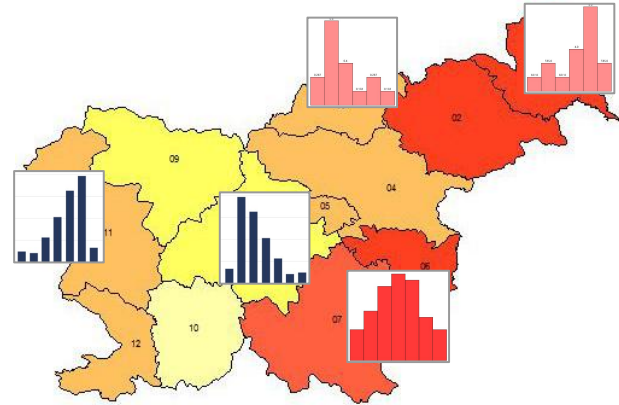
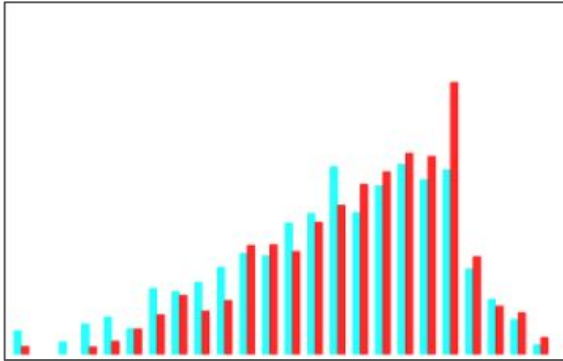
- The number of **days since the** most recent **exposure**.
- For up to last 14 days:
 - The **number of keys** that matched for an exposure detection.
 - The **highest risk score** of all exposure incidents (max 255).
 - The **highest, full-range risk score** of all user's exposures.
 - The **sum** of the full-range risk scores for all exposures for the user.

Risk score is calculated in the background < 4096



IDEA: Data only accessible to the user has value for HA

1. Actual information from the field, e.g. about social distancing (**days since exposure**), yesterday's risk encounters (**nr. of keys matched**), and yesterday's risk received (**max, sum**), can help in better management of the health crisis with less coercive measures.
2. These data can be processed **for a region**, when region label is provided by the user or for the whole country.



Health authorities now have a tool to specify the configuration settings that are used in risk score calculations and notification thresholds. Additionally, by lowering risky encounters (e.g. through efficient policies), the spread of the disease can be lowered, too.

Exposure vectors

Days since exposure													
0	1	2	3	4	5	6	7	8	9	10	11	12	13

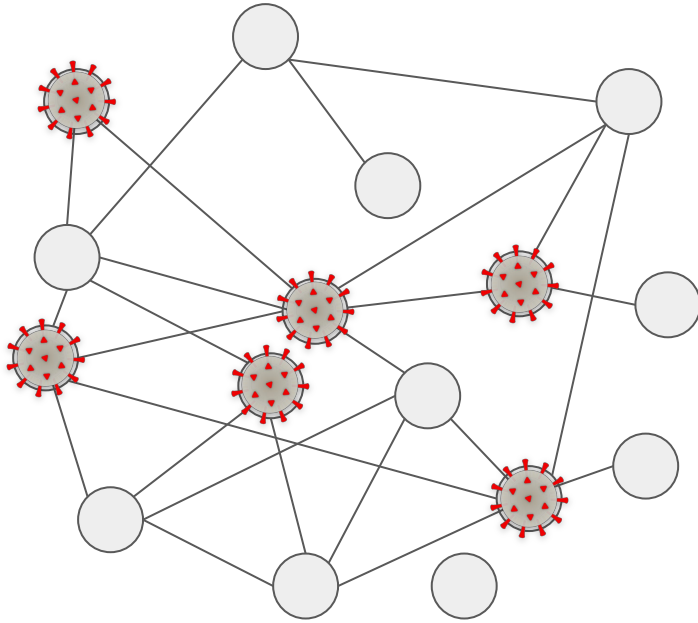
Number of keys matched *						
0	1-2	3-5	6-10	11-20	21-40	41+

Max risk received						
0	1	2	...	253	254	255

Sum risk received						
0	1	2	...			

* Estimate: 4 trips per day, 50 encounters each trip, 1% known cases are positive

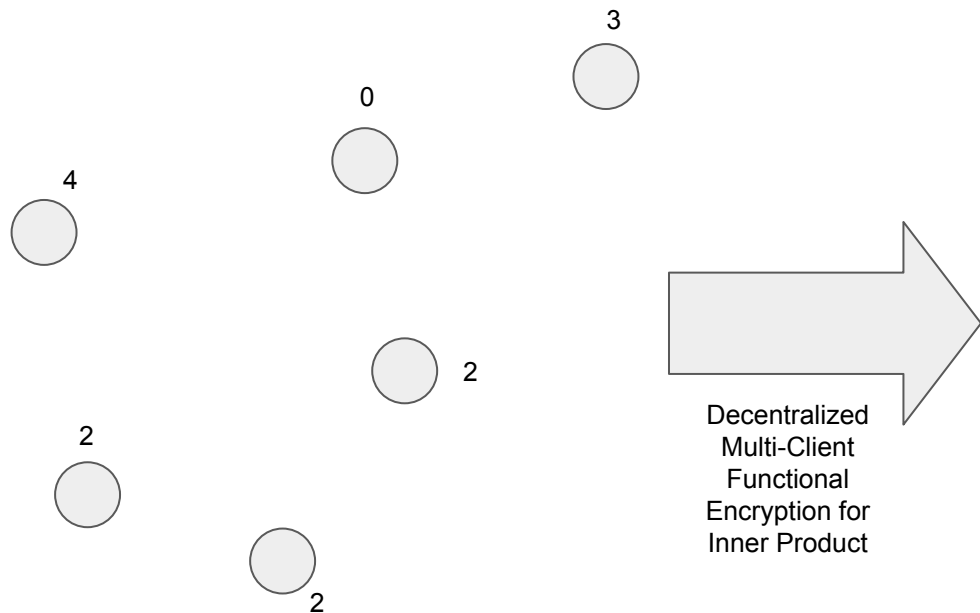
Example :: Exposure Network \Rightarrow ?



We do not have information about the exposure network's structure.

But we have all the information we need (about the exposures with the users with positive result) in the nodes.

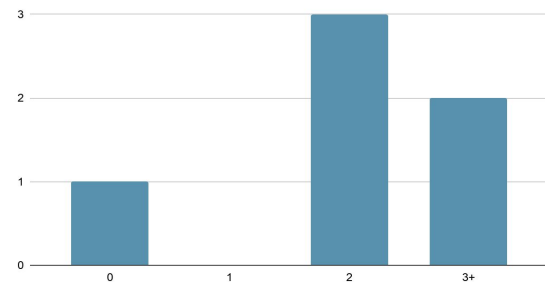
Example :: Exposure Network \Rightarrow Histogram



Analytics server

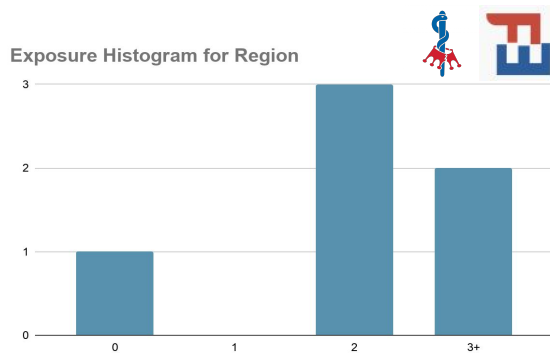
User has # contacts tested positive	Frequency
0	1
1	0
2	3
3+	2

Exposure Histogram for Region



OUR PLAN

We use FE to process the data from multiple CWA apps to get meaningful insights about exposure networks. *

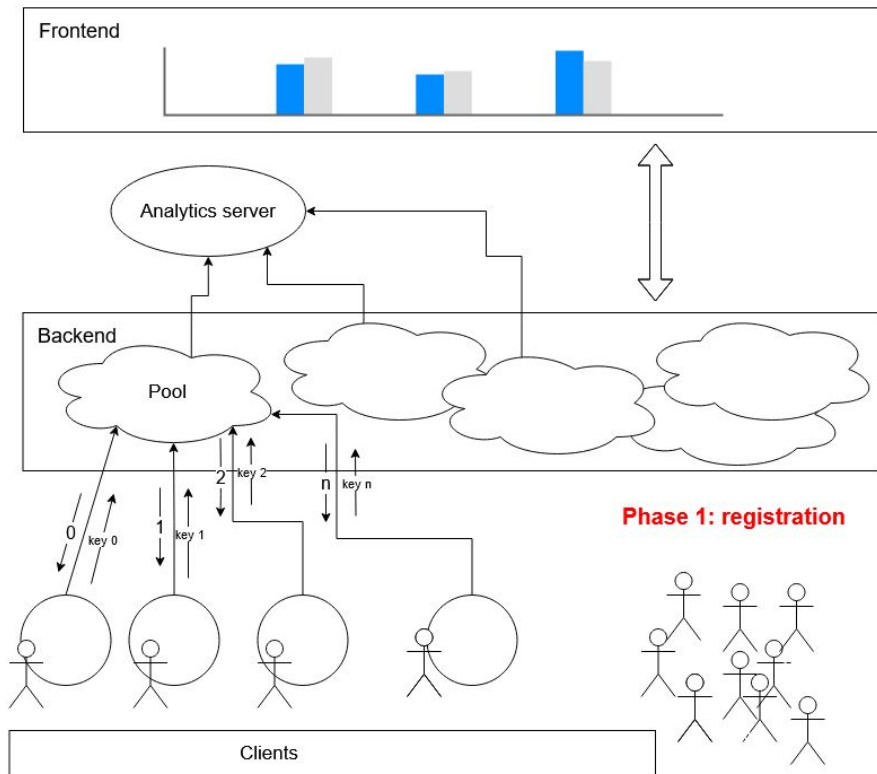


* At all steps we continue to respect data privacy and safety.



WHAT?

Phase 1: Registration

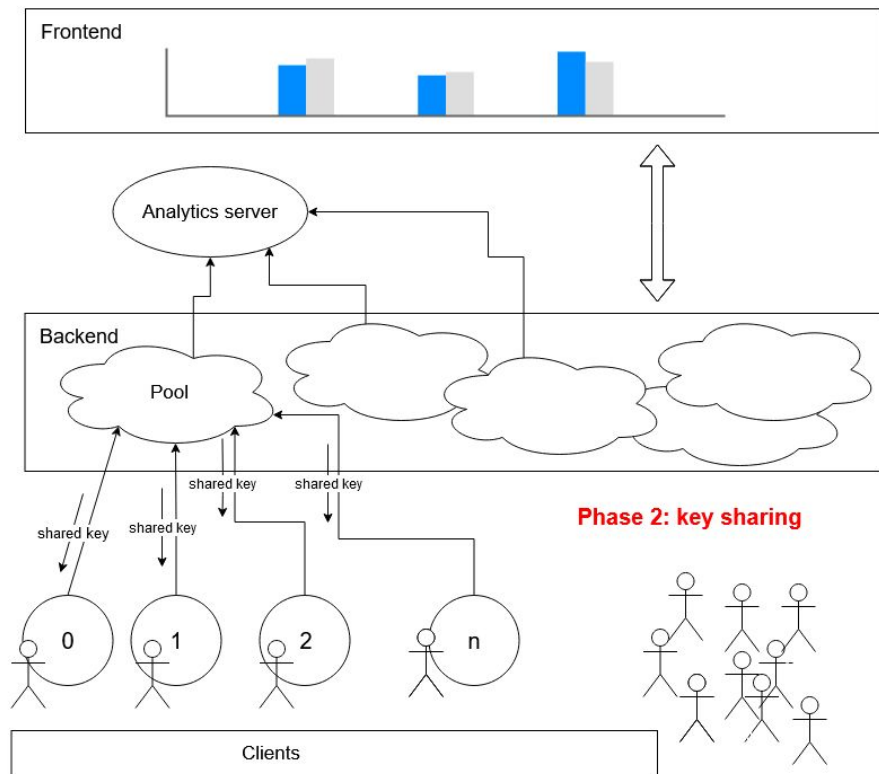


```
{
  "clientSequenceId": 2,
  "poolLabel": "2021-01-15T06:26:04.509Z",
  "registrationExpiry": "2021-01-15T06:26:34.783Z",
  "status": "REGISTRATION",
  "slotLabels": [
    "L1",
    "L2",
    "L3"
  ],
  "innerVector": [
    1,
    1,
    1,
    1,
    1
  ]
}
```

```
{
  "status": "REGISTRATION",
  "poolLabel": "2021-01-15T06:26:04.509Z",
  "poolExpiry": "2021-01-15T06:29:24.509Z",
  "creationTime": "2021-01-15T06:26:04.509Z",
  "registrationTime": null,
  "finalizationTime": null,
  "calculationTime": null,
  "publicKeys": null,
  "cypherTexts": null,
  "decryptionKeys": null,
  "slotLabels": [
    "L1",
    "L2",
    "L3"
  ],
  "innerVector": [
    1,
    1,
    1,
    1,
    1
  ],
  "histogram": "undefined"
}
```

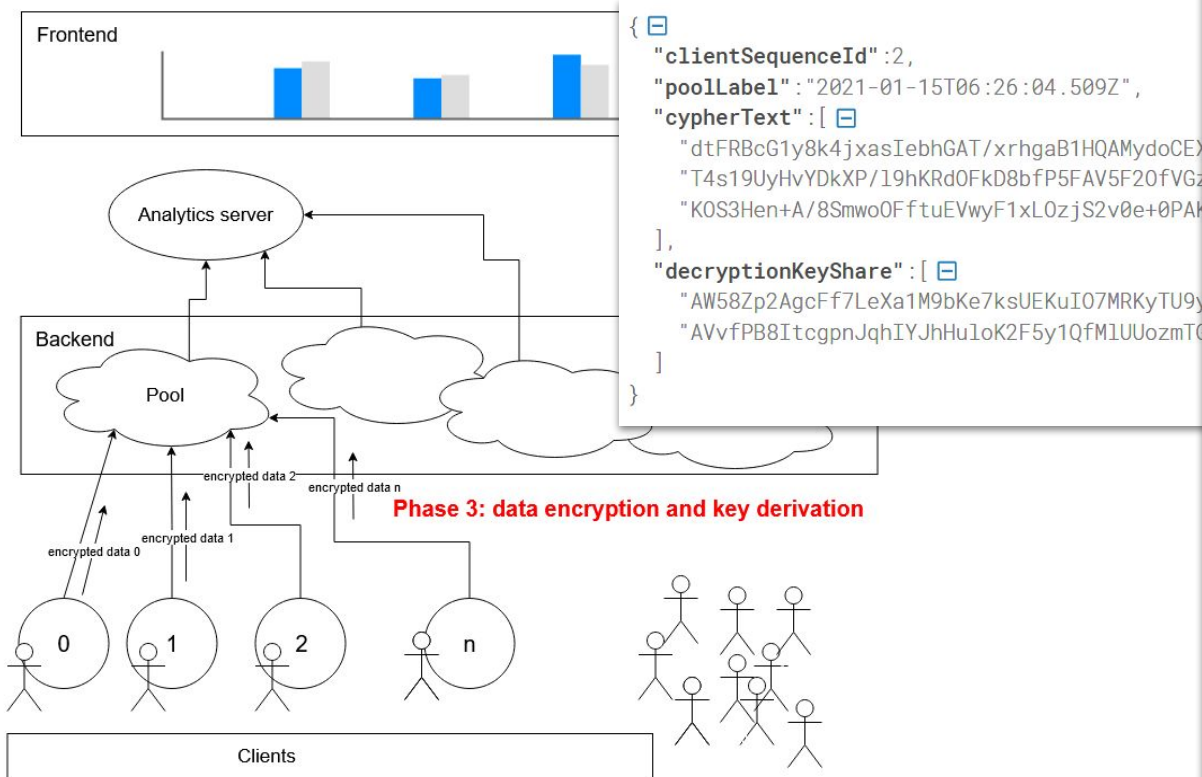
```
{
  "clientSequenceId": 2,
  "poolLabel": "2021-01-15T06:26:04.509Z",
  "registrationExpiry": "2021-01-15T06:26:34.783Z",
  "keyShare": "VKR1K0WJQ27gD10PB4XzokDfBaZ/TuvHXLNjnYKcAS"
}
```

Phase 2: Key sharing



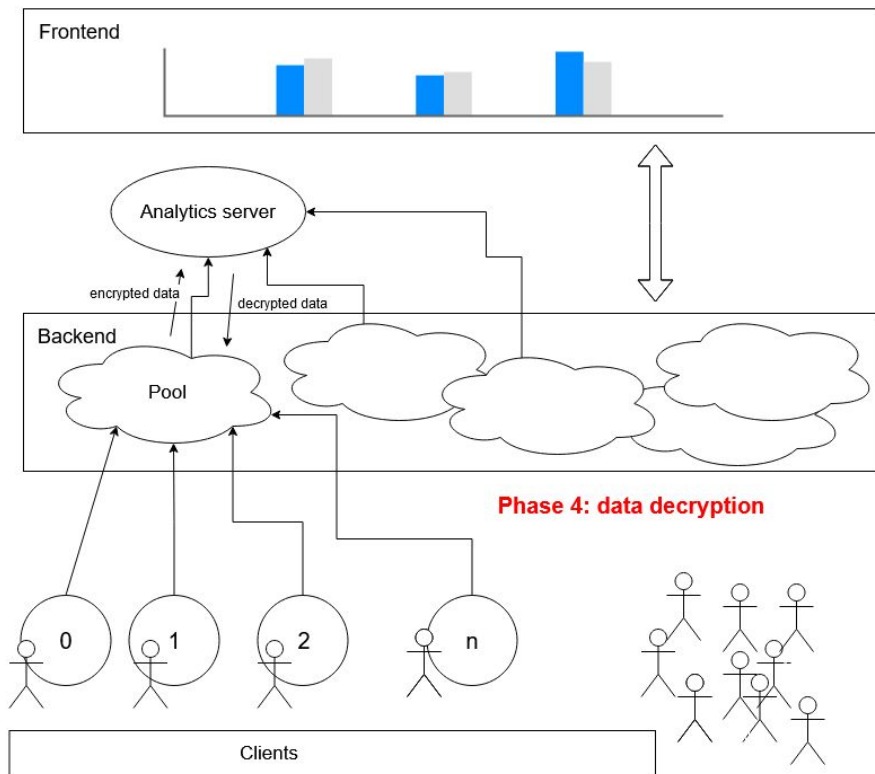
```
{
  "status": "ENCRYPTION",
  "poolLabel": "2021-01-15T06:26:04.509Z",
  "poolExpiry": "2021-01-15T06:26:15.177Z",
  "creationTime": "2021-01-15T06:26:04.509Z",
  "registrationTime": "2021-01-15T06:26:05.177Z",
  "finalizationTime": null,
  "calculationTime": null,
  "publicKeys": [
    "OfT1JeG7nHzcnJAQXQn5VTZkufXHGJE9ZYd81RB+sCtY37z7XDI",
    "PXtT9ZeAov6TKdq0QXw9jz1FmZ8B30UnDgs325s3brMJV0BPC/",
    "VKR1K0WJQ27gD10PB4XzokDfBaZ/TuvHXLNjnYKcASBW6uVSkd",
    "VPtDkLdYa21zBuWFphUqVNUKZFe68yXMBX3MCKQ770d1Wp0e+H",
    "CQ74zMbJwMXCd/4igW3B4JjQJTz1S0gCFw1WJtMvt6Q+81bRfr"
  ],
  "cypherTexts": null,
  "decryptionKeys": null,
  "slotLabels": [
    "+"
  ],
  "innerVector": [
    "+"
  ],
  "histogram": "undefined"
}
```

Phase 3: Data encryption



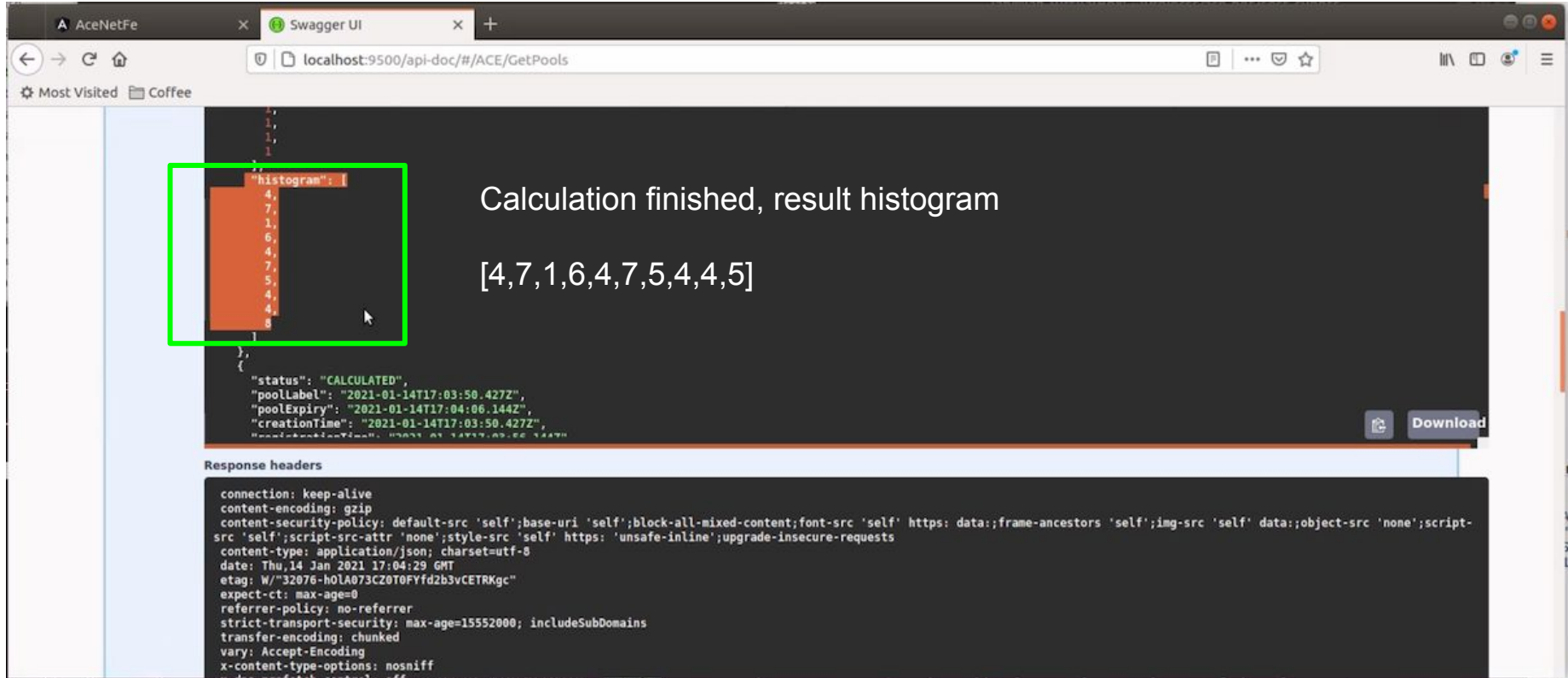
```
{
  "status": "FINALIZED",
  "poolLabel": "2021-01-15T06:26:04.509Z",
  "poolExpiry": "2021-01-15T06:26:15.177Z",
  "creationTime": "2021-01-15T06:26:04.509Z",
  "registrationTime": "2021-01-15T06:26:05.177Z",
  "finalizationTime": "2021-01-15T06:26:07.908Z",
  "calculationTime": null,
  "publicKeys": [
    [
      "c3UGPl0Q2W0wwsdQkIz8MZ5lw3xU2ihHqrRf2o/YvJlqBG",
      "iM/UKFVjbSZz+7mDmsMsYYAU8GtSkGHxCED+610W1AAT68",
      "X1VB1fTs/StR5ViLAeDCnIf/DbX3xcUsC8qWSBirb8U/YQ"
    ],
    [
      ],
    [
      ],
    [
      ],
    [
      ]
  ],
  "decryptionKeys": [
    [
      "ATDhn617K0U3l60oDUiZkARU8i2fnYNsFa//5/6DDCWhk",
      "ARlbtE/wCscBHsYlhU5HbHl/BQlyDG4HHow4KvF0CBOfRj"
    ],
    [
      ],
    [
      ],
    [
      ],
    [
      ]
  ],
  "slotLabels": [
    ],
  "innerVector": [
    ],
  "histogram": "undefined"
}
```


Phase 4: Data decryption



```
{
  "status": "CALCULATED",
  "poolLabel": "2021-01-15T06:26:04.509Z",
  "poolExpiry": "2021-01-15T06:26:15.177Z",
  "creationTime": "2021-01-15T06:26:04.509Z",
  "registrationTime": "2021-01-15T06:26:05.177Z",
  "finalizationTime": "2021-01-15T06:26:07.908Z",
  "calculationTime": "2021-01-15T06:26:09.188Z",
  "publicKeys": [ + ],
  "cypherTexts": [ + ],
  "decryptionKeys": [ + ],
  "slotLabels": [ + ],
  "innerVector": [ + ],
  "histogram": [
    2,
    1,
    2
  ]
}
```

Analytics server (access via API through Swagger)



Swagger UI

localhost:9500/api-doc/#/ACE/GetPools

Most Visited Coffee

Calculation finished, result histogram

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

Response headers


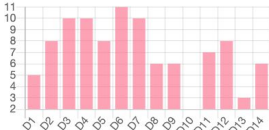

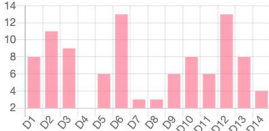
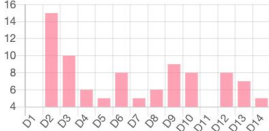

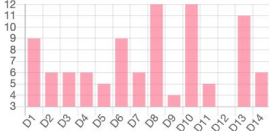
```
connection: keep-alive
content-encoding: gzip
content-security-policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https; data:;frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https; 'unsafe-inline';upgrade-insecure-requests
content-type: application/json; charset=utf-8
date: Thu, 14 Jan 2021 17:04:29 GMT
etag: W/"32076-h0LA073C20T0FYfd2b3vCETRGc"
expect-ct: max-age=0
referrer-policy: no-referrer
strict-transport-security: max-age=15552000; includeSubDomains
transfer-encoding: chunked
vary: Accept-Encoding
x-content-type-options: nosniff
```

Front end

A^oE* - Analytics on Covid Exposure Networks

Pool overview (5)

Reset

Status	Size	#PubKey Shrs	#Cyphertexts	Region	#Days since last exposure
CALCULATED	100	100	100	 Gorenjska	
CALCULATED	100	100	100	 Zasavska	
CALCULATED	100	100	100	 Goriška	
CALCULATED	100	100	100	 Jugovzhodna Slovenija	

WebSocket communication with the analytics server in real-time.

Server, clients, histograms etc. are configurable.



DEMO

Interesting links

- FE
 - Decentralized Multi-Client Functional Encryption for Inner Product <https://eprint.iacr.org/2017/989.pdf>
 - Subway heatmap <https://github.com/fentec-project/FE-anonymous-heatmap>, paper: <https://fentec.eu/content/privacy-enhanced-machine-learning-functional-encryption>
- COVID
 - COVID-19 Tracker, <https://covid-19.sledilnik.org>
 - Understanding metropolitan patterns of daily encounters, https://www.researchgate.net/publication/235009037_Understanding_metropolitan_patterns_of_daily_encounters
 - Slovenian Temporary Exposure Keys, <https://github.com/sledilnik/cwa-scrape>
- Corona-Warn-APP
 - Corona-Warn-App, <https://www.coronawarn.app>, <https://github.com/corona-warn-app/cwa-documentation>
 - CWA Solution Architecture, https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md
 - Exposure notification framework for contact tracing <https://covid19.apple.com/contacttracing>, <https://www.google.com/covid19/exposurenotifications>
 - Exposure Notification cryptography specification, https://blog.google/documents/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf
 - CWA Risk score calculation, <https://www.r-bloggers.com/2020/09/risk-scoring-in-digital-contact-tracing-apps>
- Contact tracing
 - Kukkala VB, Saini JS, Iyengar SRS, Privacy preserving network analysis of distributed social networks <https://eprint.iacr.org/2016/427.pdf>
 - Kukkala VB, Iyengar SRS, Computing Betweenness Centrality: An Efficient Privacy-Preserving Approach https://link.springer.com/chapter/10.1007/978-3-030-00434-7_2
 - Kukkala VB, Iyengar SRS, Identifying Influential Spreaders in a Social Network (While Preserving Privacy, <https://content.sciendo.com/downloadpdf/journals/popets/2020/2/article-p537.pdf>

Possible extensions

- Bring the results of this project to Corona-Warn-App
- “Those who count the votes decide everything” - Voting systems (giving N votes between $M \geq N$ options)
- Randomising communication patterns, by involving a part (half?) of the requests to be ignored or by submitting data using secret sharing schemes (e.g. partial data, multiple times)
- GoFE problem: "panic: runtime error: invalid memory address or nil pointer dereference [signal SIGSEGV: segmentation violation code=0x1 addr=0x10 pc=0x67689b]"