PriLock: Citizen-protecting distributed epidemic tracing
PRELIMINARY DESIGN V.1.0

Paulo Esteves-Verissimo, Jérémie Decouchant, Marcus Völp, Alireza Esfahani, Rafal Graczyk
SnT - Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg
Email: paulo.verissimo@uni.lu, jeremie.decouchant@uni.lu, marcus.voelp@uni.lu, alireza.esfahani@uni.lu, rafal.graczyk@uni.lu

May 12, 2020

Abstract

Contact tracing is an important instrument for national health services to fight epidemics. As part of the COVID-19 situation, many proposals have been made for scaling up contract tracing capacities with the help of smartphone applications, an important but highly critical endeavor due to the privacy risks involved in such solutions. Extending our previously expressed concern, we clearly articulate in this article, the functional and non-functional requirements that any solution has to meet, when striving to serve, not mere collections of individuals, but the whole of a nation, as required in face of such potentially dangerous epidemics. We present a critical information infrastructure, PriLock, a fully-open preliminary architecture proposal and design draft for privacy preserving contact tracing, which we believe can be constructed in a way to fulfill the former requirements. Our architecture leverages the existing regulated mobile communication infrastructure and builds upon the concept of "checks and balances", requiring a majority of independent players to agree to effect any operation on it, thus preventing abuse of the highly sensitive information that must be collected and processed for efficient contact tracing. This is enforced with a largely decentralised layout and highly resilient state-of-the-art technology, which we explain in the paper, finishing by giving a security, dependability and resilience analysis, showing how it meets the defined requirements, even while the infrastructure is under attack.

1 Introduction

In an earlier text published on LinkedIn[1], we justified the reasons behind our belief that a national infrastructure is indispensable to attend to the needs of nations in the presence of threats posed by modern pathological agents, of which COVID-19 is but an example of the future, and — according to specialists — perhaps a mild one. Contact tracing (CT), that is the systematic identification of potentially infected individuals by tracing and testing those that had been in contact with a known infected person and where a transmission of the virus may have happened, has been an effective measure to confine the COVID-19 outbreak in the early phase after new year, but ceased to be effective the moment NHS tracing capacities got exhausted. Aside from COVID-19, the effectiveness of CT has been demonstrated in many outbreaks [17, 37, 29, 18]. For example, WHO reports the essential role of CT in controlling Ebola outbreaks in Africa[2]. The goal of digital contact tracing[3] is to automate CT and as such increase NHS tracing capacities by several orders of magnitude to extend the time when CT remains effective in chasing exponentially

[1] https://www.linkedin.com/pulse/citizen-protecting-proximity-tracing-covid-19-between-paulo
[2] https://www.who.int/csr/disease/ebola/training/contact-tracing/en/
[3] https://science.sciencemag.org/content/sci/early/2020/03/30/science.abb6936.full.pdf

growing infection rates. However, such a proposal should preserve fundamental needs and goals, some of which hard to reconcile, such as efficiency and effectiveness, as well as coverage, fairness and privacy for population.

Surprisingly or not, most of the recent debate has been centred around cryptographic aspects. However, we believe this to be a *distributed critical information systems* problem at its centre. Only by treating it with the relevant body of knowledge will we reach the goals. By this, we mean the right combination of s.o.t.a. ICT technologies (distributed algorithms, fault and intrusion tolerance, networking and cloud technology, cryptography), guided by requirements from the several societal sectors, not only national health services and epidemiologists, but also economists, for example.

We propose the architecture of **PriLock: Citizen-protecting distributed epidemic tracing**, a critical information infrastructure (CII). The values we wish to safeguard in the design we make public, are:

- **Maximizing nation-wide coverage of people and territory**
- **Ensuring near real-time situational awareness through whole epidemic life cycles**
- **Transparent protection of citizens' rights, not just privacy, but also inclusiveness and fairness.**
- **Resilience against data- and system-based social and technical threats.**
- **Preservation of digital sovereignty.**
- **Protection of economy by precise and selective throttling (closing and opening).**

In a nutshell, PriLock should be oriented at the protection of populations, cities, countries, trans-border regions, in the face of epidemics. The objectives outlined above imply the participation of a plurality of stakeholders, and for effectiveness, should leverage on existing CIIs, such as the NHS systems and the Telco networks, both of which regulated sectors. This preliminary proposal attempts at giving guidance to architects and designers of infrastructures, about design avenues for devising a citizen-protecting distributed epidemic tracing critical information infrastructure.

A CII of this kind is logically centralised in nature. However, in distributed systems logical centralisation does not necessarily imply monopolist trust models, or physical centralisation. Nor decentralisation or peer-to-peer prevent abuses per se. Both misconceptions have been part of recent debates[4][5][6]. The PriLock architecture follows best practices in distributed and resilient critical information systems design. It uses geographical decentralisation to reduce the baseline threat plane, both at the periphery and at the core. Its management trust model does not follow a centralised, monopolist philosophy, but a consensual one, where abuse is technically prevented since no operation can be executed by single or minority groups of entities, and all critical operations require intervention of a quorum of the (independent) entrusted entities ("checks and balances").

The core facilities themselves are also largely decentralised, distributed and/or replicated at the entrusted entities sites. However, this PriLock network of components establishes perimeter isolation from the legacy systems, with very clear entry/exit points. This isolation is strengthened with defence-in-depth mechanisms implementing a high degree of fault and intrusion tolerance. The resulting threat plane reduction in face of external and internal attacks or faults is a key aspect, to achieve resilience in general, and privacy in particular, despite handling critical data.

[4] https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/
[5] https://eprint.iacr.org/2020/399.pdf
[6] https://nadim.computer/posts/2020-04-17-pepppt.html

Unlike some recently published approaches (e.g., exclusively based on Bluetooth), we favour technologies that promote incremental inclusion of all population strata — economic, literacy or age. As such, we see currently no alternative to the mobile communication system as a baseline. We aim as well at protecting digital sovereignty, avoiding as much as possible solutions that open considerable threat planes like those affecting phone-to-phone attacks or generating inconsiderate dependence on phone/OS vendors, which might for example cause massive leakage of national critical data to unidentified threat actors. Finally, we consider that only a global approach can provide the accuracy and near real-time timeliness of information required for a low risk, high effectiveness throttling of the economy.

In a nutshell, our proposal attempts at **striking a balance between securing health, protecting privacy and safeguarding the economy.**

2 Requirements specification

To be clear about the objectives and trade-offs of PriLock, we discuss below all the desirable requirements that we believe should be met by an infrastructure of this kind, and the rationale for meeting them.

2.1 Desirable objectives and implied requirements

We list the almost indispensable functional objectives that should be reached by any nation-level critical infrastructure doing digital contact tracing (CT) (R1-R6):

R1 Be epidemic-agnostic: able to act on any epidemic, even the unexpected, in near real-time.

R2 Help find the highest possible rate of infected individuals in near real-time.

R3 Help find reasonably complete and accurate potential infection chains in near real-time.

R4 Alert, monitor, confine, and trace potentially infected individuals in near real-time.

R5 Diagnose country/region/community epidemic dynamics in near real-time (map basic infection evolution numbers; locate and map infection hotspots and trajectories; detect super infectors and/or lone wolves; predict collections of asymptomatic individuals; discern between external and communal infection paths).

R6 Incorporate lessons and feedback from first epidemic outbreaks and adapt further actions during individual re-infections and epidemic recurrences, in near real-time.

Additionally, the following non-functional objectives should be met (R7-R10):

R7 Guarantees of protecting citizens' fundamental rights (such as transparency, privacy and equality) in compliance with the law.

R8 Resilience to manipulation and forging, fake-news, gossip, panic, denial of service.

R9 Sustained real-time capability under overload, to maintain situational analysis and reaction capacity (infection roadblocks; sanitary fences around hotspots; group quarantines; and later, precise selective re-opening).

R10 Smoothly incremental accuracy and recall of proximity event determination, from an inclusive though possibly coarse sovereign nation-wide baseline technology level, to finer levels attainable by s.o.t.a. technology (not only but including 5G).

2.2 Rationale

If those requirements are met, we are bound to have a CII (critical information infrastructure) that really serves a nation and its individuals, in the possibly hard times to come in the next years[7]. Furthermore, their correct implementation guarantees that the 7 fundamental principles of the GDPR [19] are followed: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

The possible criticality and magnitude of future epidemic surges advises that nations be prepared: instead of reactive, be proactive. Moreover, the time is now, and not during the next epidemic surge.

We believe this is a task for the ***state***, as one stakeholder of the nation. It should have the important responsibility (political as well as economic) of its implementation and operation, relying on other stakeholders (regulated companies, regulators, public associations, for example).

However, the ***people***, individuals or collections thereof (who 'are' the nation) have a right to enjoy the CII on an equal basis (regardless of their technical literacy), release PII (personally identifiable information) lawfully, only on a need basis, by the principles of storage limitation and data minimisation, and having transparent access to its design and operation auditing.

It would be excellent if no involvement of PII would be needed, given the criticality, but such an infrastructure, if it is to protect the nation, it must get to the nation.

There are currently a number of proposals for digital contact tracing, including DP3T[8], TraceTogether, ROBERT[9], TCN[10], NTK[11], Canetti-Trachtenberg-Varia [9], the Apple/Google's joint initiative for Bluetooth distance measurement in iOS/Android[12], Pronto-C2 [4], PACT-WEST [11], PACT-EAST [13], Reichert-Brack-Scheuermann [33], etc., which we do not wish to criticize negatively, since all contributions are not too many in these critical times. We believe nevertheless that a good test of their fitness for the purpose would be for the authors showing that they pass the Litmus test of meeting the requirements R1-10 above. Some proposals, however focused, present very elegant algorithmic solutions to parts of the big picture addressed by PriLock. We should not exclude the possibility of considering their contribution.

In this sense, we believe that approaches ***peer-to-peer managed*** (actually or pseudo-decentralised), ***and voluntarist*** (totally or mostly based on word-of-mouth gossip), will work to a certain point, but will miss some important objectives of the list above, not least, the equality of access and coverage of population, and the capacity for global (nation-wide) reasoning. However, approaches ***centrally managed*** (single entity), and ***top-down controlled*** (totally or mostly based on the «Trust me because I tell you to!» principle), and as such ***opaque***, will work as well, but miss another set of equally important objectives listed, not least, by losing confidence of the people in terms of privacy, and perpetuating a state of surveillance.

It is our opinion that the risks impending on the PII can be significantly mitigated, with an adequate mix of the right social/political management framework and state-of-the-art technical measures to safeguard the information. This being achieved, the benefits (R1-10) will largely outweigh the risks.

An infrastructure such as we envisage, albeit supported by the state, must not be built or managed in a fully centralised way. It should instead be managed in concertation through ***consensual actions by several powers exerting mutual control*** ("checks and balances"), in respect for the PII it will store and process. Correctness of these consensual actions must of course be technically enforced by robust technologies, such as protocols of the BFT class

[7] `https://www.newyorker.com/news/daily-comment/the-pandemic-isnt-a-black-swan-but-a-portent-of-a-more-fragile-global-system`

[8] https://github.com/DP-3T/documents

[9] https://github.com/ROBERT-proximity-tracing/documents

[10] https://tcn-coalition.org/

[11] https://github.com/pepp-pt

[12] https://www.apple.com/covid19/contacttracing/

[13] https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf

(Byzantine Fault Tolerance), playing together with multiparty cryptography protocols. These technologies, albeit sophisticated, have today a high technology readiness level (TRL), spawned by its increasing use in a number of real workd applications, notably the Fintech/Blockchain area.

Furthermore, the infrastructure should be dormant (locked and largely empty of information) most of the time, only to be activated in times of need, by multiparty decisions; PII information collected should be disposed of immediately it is no longer needed; PII information at rest during active periods should be protected with strong multiparty cryptography, and so forth. In consequence, such an infrastructure must be designed and implemented using the best technical practices available to ensure all these objectives.

For this to be done without large impact on the efficiency, the decision and operation processes should be streamlined and based on IT-supported workflows, but attested and certified continuously (e.g., by indelible logging apparatus and/or blockchain supported ledgers). Ex-ante and ex-post auditing should be put in place, effected by an independent regulation body. Citizens should as well have transparent access to the modus operandi and the results of the regulation actions.

3 Preliminary Architecture and Draft Design

We present a fully-open Preliminary Architecture Proposal and Draft Design of PriLock. Our purpose is not to give a fully-fledged design, but rather to give guidance to architects and designers of such infrastructures, should these ideas merit the support of the main stakeholders in a nation, certainly the state and the citizens. As such, we do not intend to go into too much further detail in the sections below, beyond giving the outline and skeleton of protocols and mechanisms, showing that the main architectural, data model and algorithmic design options meet the requirements R1-R10. The design is also open enough that, within the margin we leave for the technical options, different nations may strike different balances between securing health, protecting privacy and safeguarding the economy.

3.1 Introduction

Generically, the PriLock infrastructure is implemented and controlled by a "Federation for Epidemic Surges Protection- *EpiProtect* ". In the context of this paper, *EpiProtect* is the designation of the necessary coalition of interest formed by entities of the state — such as relevant government ministries, National Health Service entities like centres for disease control and hospitals, Justice, an independent Regulation body for the CII — and regulated companies, regulators, research and technology institutes and universities, public associations, for example. The PriLock infrastructure, albeit supported by the state, is managed not in a fully centralised way, but in concertation, by several powers exerting mutual control ("checks and balances"), in respect for the PII it will store and process. In essence, the PriLock Entrusted Authorities (*PEA*) is a subset of the entities listed above, whose number and quality/role will depend on specific countries' culture and legal systems. *PEA* members are those that can collectively issue authorisations for the manipulation of PriLock. As seen below, all such operations must be vetted by a quorum of the *PEA*. Other entities such as listed above will be PriLock-Associated Entities (*ASE*).

3.2 Architecture components

Figure 1 gives an overview of the architecture. It is worth noting that, following a successful concept in previous research on critical information infrastructures, the technology required is already available (e.g., but not exclusively from the EU projects CRUTIAL[14], MASSIF[15], BBC[16], SEGRID[17]). PriLock attempts at leveraging (rather than replacing or duplicating) existing CIIs, in this case the legacy Telco and Public Administration infrastructures in general, and the Mobile Communication system in particular. As such, as seen in the Figure, whilst the existing legacy systems are represented in brown, PriLock is laid out as an overlay architecture over them, represented in blue. Furthermore, to ease integration and cause minimal disturbance, PriLock components are highly modular and self contained (information switches, cloud subsystems). This perimeter isolation with very clear entry/exit points (boundaries between brown and blue in the Figure) is also key to security and dependability. As we show ahead, it is strengthened with other defence-in-depth mechanisms in order to attain the very high levels of resilience desired.

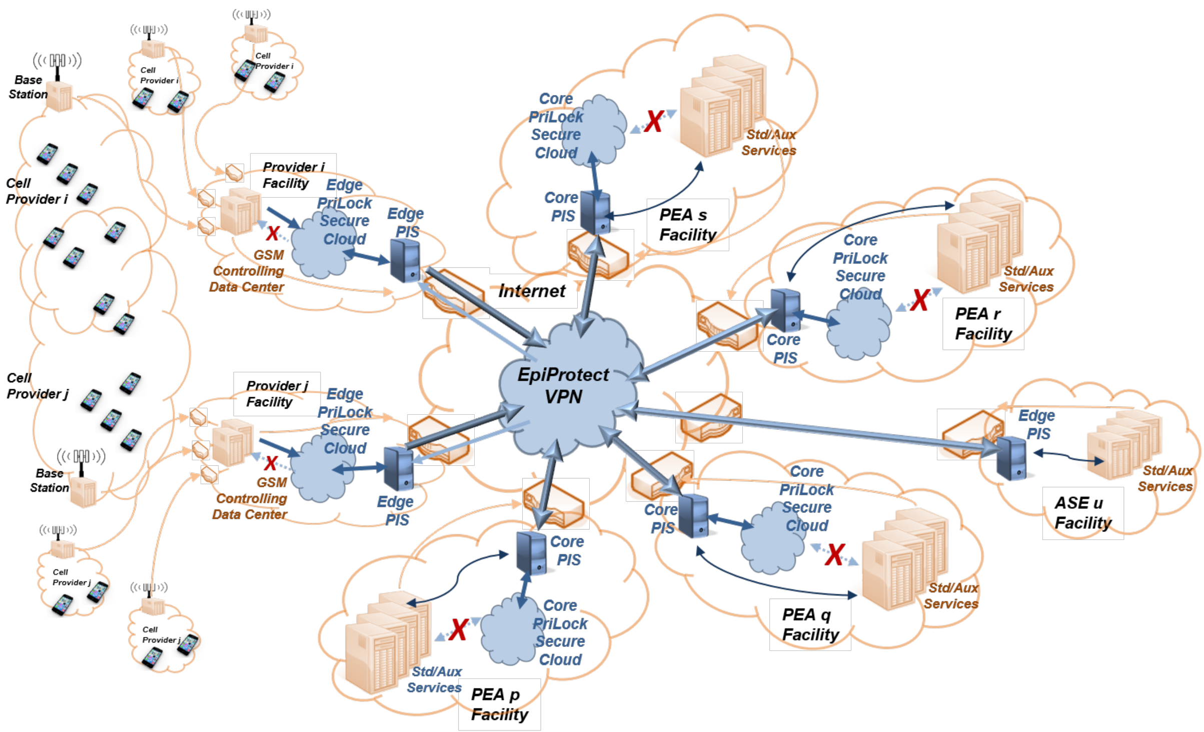

Figure 1: PriLock architecture

3.2.1 Edge realm

Telco Operator and Service Provider (Provider in short) cellular network cells such as macrocells, microcells, picocells, and femtocells (existing).

We leverage the existence of the cellular public network, since any 'live' mobile phone will be in contact with at least one Provider (or potentially more, in case of roaming), in any covered location. PriLock is set up as an overlay architecture over/aside the cellular systems, and tries to cause the least disturbance possible on the cellular network. However, we consider that PriLock, as a regulated infrastructure of public interest, may reasonably imply some minimal changes on the Providers, as described below.

[14] https://cordis.europa.eu/project/id/848109
[15] https://cordis.europa.eu/project/id/257475
[16] https://cordis.europa.eu/project/id/317871
[17] https://cordis.europa.eu/project/id/607109

Currently, the cellular network has a degree of variation in the implementations, according to Providers' structure and xG generation. In what follows, we provide a general outline of a prototypical architecture, for simplicity and without loss of generality. In cellular networks, small cells are employed to enhance the link quality and network capacity [31]. Several types of small cells include femtocells, picocells, microcells, and macrocells – broadly increasing in size from femtocells which are the smallest, to macrocells which are the largest. The network is normally organised in cells, nominally covering a geographical region, by sets of antennas controlled by the cell Base Station. Cells from the same provider, or from different providers, overlap in their spatial coverage.

The Figure 2 suggests the current reality of the cellular (mobile communications) system, and the small add-ons that may be implanted by PriLock (fBS in blue, explained below). Macrocells (standard cells and microcells) implement the external (street) structure, respectively by macrocell Base Stations, mBS. Communication inside premises (e.g., internal parkings, theatres, shopping malls) is secured by additional, finer granularity, picocells, from a given provider, controlled respectively by picocell Base Stations, pBS. These are aggregated under the realm of the macrocell that subtends them, by a hierarchical logical structure, called paging cell. The useful ranges of the pBS of a same paging cell partially overlap in their spatial coverage. A phone will register to a cell upon arrival (e.g., through the macrocell base station mBS), and after that the communication enters stand-by listening mode to save energy. From then on it can be paged by any of the base stations in that paging cell (e.g., walking through a shopping mall) on a need basis (e.g. an incoming call or SMS).

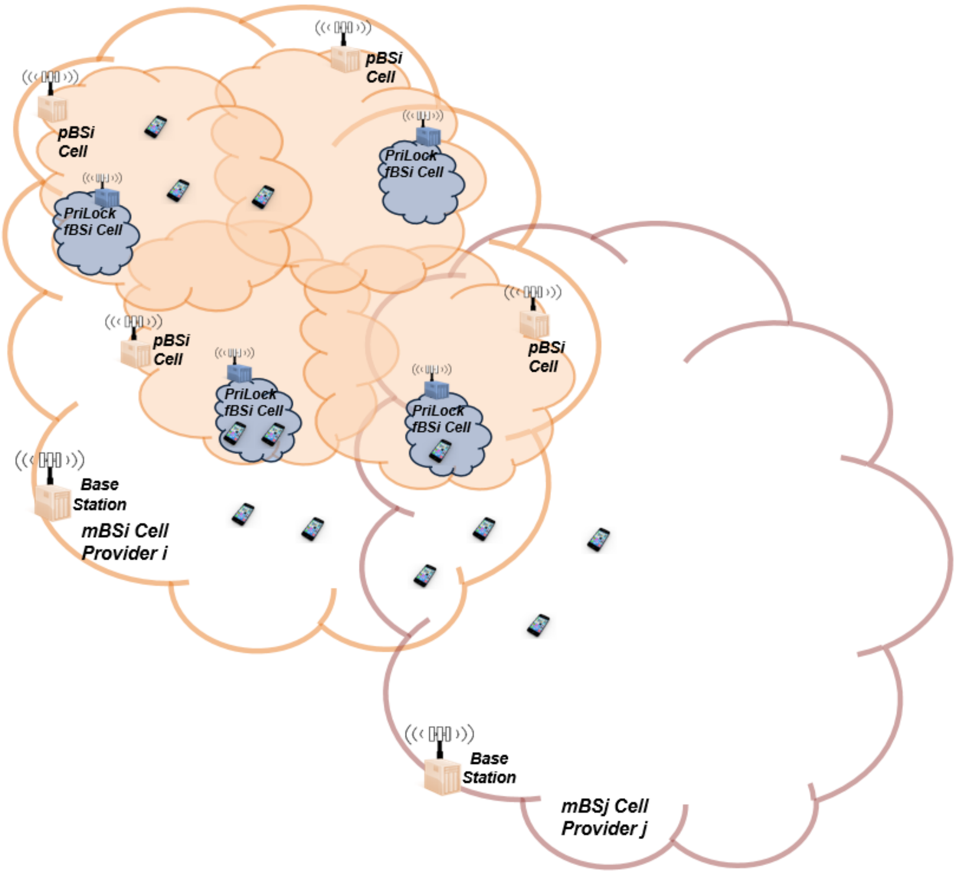

Figure 2: PriLock integration with cellular network infrastructure

The information flow will be detailed in a later section, but a key data structure for the process described below is introduced now: *Proximity Detail Record (PDR)* — containing, for each region (cell), the timestamps of contiguous periods of time spent in the region by a phone, the average proximity vector from the centroid, plus an encoded ID of the region BS.

Technically, it is possible today that:

(i) mBS or pBS calculate the proximity of a phone to the centroid of the users distribution of the respective antenna set, as a relative position;

(ii) several pBS of a paging cell can periodically page a phone on purpose to determine that proximity vector (e.g., a polar coordinate from the centroid) and generate a PDR;

(iii) the mBS and several pBS of a paging cell can triangulate their space-time readings of proximity of a same phone, in order to get a much more precise value of the relative position of the phone relative to the antenna set, and create the respective more precise PDR;

(iv) in alternative, that triangulation can be performed later, over independently recorded PDR registers by several BS, containing space-time readings of proximity of a same phone to those BS, relative to a similar time interval;

(v) none of these registers need to contain absolute location information.

Edge Telco Provider Cellular Controlling Data Center (existing).
We denote the cellular Controlling Data Centers (DC) generically (provider implementations vary), as the first DC on the edge of the provider network where PDRs collected by the base station network can be concentrated and stored systematically.

Edge PriLock Secure Cloud (PSC) (in Telco Provider Cellular Controlling Data Centers).
The Edge PriLock Secure Clouds (PSC) are the PriLock-supplied subsystems co-located in each Controlling Data Center of Providers. The PDRs are stored encrypted in this installation as they come from the BS, by the Provider, which has a write-only (push) interface to the Secure Cloud. After PDRs are stored in the cloud, they can no longer be accessed by the provider.

Edge PriLock Information Switches (Edge PIS) (containing the edge services and connection to the VPN).
The Edge PIS are the points of contact of the edge secure clouds with the core systems, through the *EpiProtect* VPN (see below). They also run services that manage the information in the secure cloud. We foresee that these data secure the principles of data minimization and storage limitation followed by data protection authorities and the GDPR in general, by: containing minimal information about phones only; ibid about presence under cellular network cells, i.e. relative location, i.e. proximity, not absolute location; being automatically deleted after a time-to-live period to be defined, a function of the target disease incubation time.

3.2.2 BASE 0 - Proximity Tracing with Cellular components

Proximity Tracing with cellular components has incremental levels of precision, from older xG or e.g. rural areas where the useful range of mBS may be kilometers, through metropolitan areas where it may be a couple dozen meters or less, to inside premises pBS, where it can come down to a few meters. This approach shows a virtuous adaptation of accuracy to human density, providing a predictable rate of false positives grossly proportional to predicted urban density. The approach also promotes inclusion, since: 30% of the population is estimated not to own a smartphone, and most older people are not tech-savvy. Thus, including older people in a system that works automatically for them, and with a predictable rate of false positives grossly proportional to age (and thus health risk) and tech-illiteracy, seems as well a virtuous trade-off for an infrastructure of public interest. From the viewpoint of the national interest, it is also the one offering better reliability, security and sovereignty conditions for a start, since it does not suffer from the considerable threat plane affecting phone-to-phone attacks, or the phone/OS vendor interference (both in GPS and in Bluetooth sensing).

Experiments will need to be done to determine the actual levels of accuracy and recall of contact tracing allowed by the several technical levels of the baseline system (mBS, pBS, triangulation) as we have described.

Some things should be noted however: (i) the problem with older generation equipment is expected to lie mostly with accuracy, i.e. in alerting too many people, rather than missing infected/infector people; (ii) if our conjecture is correct, this would concern the virtuous combinations mentioned above and thus be a good trade-off; (iii) on the other hand, accuracy will be most important in points likely to become infection hotspots (packed-layout restaurants and other commercial surfaces, bars, theatres, sports halls, PoS, etc.), where again, newer generation equipment is more expected; (iv) next we discuss ways to further improve accuracy thinking about these spots.

3.2.3 BASE 1 - Proximity Tracing with Cellular Enhanced components

PriLock cells.
We go further in solving this remaining problem and improving the precision and accuracy of contact tracing given by this baseline architecture, by selectively enhancing them in the most needed points (as the examples just above). We go down one order of magnitude in spatial range, inspired by the femtocell principle in mobile networks. Femtocell is a small, low-power low-capacity base station, with a useful range of a few meters, typically designed to solve coverage corner cases, or serve homes or small businesses.

The analogy stops there, and we introduce PriLock special femtocells (depicted in blue in the Figure 2), implemented and controlled by dummy base stations that we call fBS. Inside a given paging cell, there may be several fBS, installed in consonance with the respective Provider. fBS present themselves to phones as genuine base stations of a paging cell. So they can force the periodical paging of a phone in the (very small) area of their useful range. After each ping, they do not perform mobile communication, which is ensured by having the phone connect to another pBS in the area with overlapping coverage.

Technically, it is possible that mBS and pBS are software-enhanced (with few exceptions) so that fBS can interact with mBS and pBS nearby in a simple manner:

(i) by having them calculate and store the proximity of the fBS the same way they do with phones, triangulating their space-time readings in order to get a precise value of the relative position of the fBS relative to the antenna set (this operation is done once per fBS set-up, since the fBS is not expected to move relative to the mobile system BSs, in principle);

(ii) whenever this is not possible, the fBS can be georeferenced by hand through a GIS of the area.

(iii) by sending the related paging events of phones that enter and leave their range to one of the mBS or pBS (which issue a PDR with the respective timestamps, the average proximity vector of the fBS from the centroid of the issuing BS, and an encoded ID of the latter). The PDR thus contains a point with much higher precision than what is achieved even by picocells.

Alternative proximity tracing technologies.
PriLock assumes a default baseline measurement approach based on the cellular apparatus, for inclusion, fairness and completeness. Then, it improves on the baseline through the above-mentioned described PriLock pseudo femtocell.

However, it welcomes integration of other approaches, for example those working on a voluntary basis, possibly for complementing information in specific situations and areas, e.g., GPS, Bluetooth, Wifi or other.

However, this must be done with care, always taking into account the non-functional objectives (R7-R10), in particular digital sovereignty.

3.2.4 Virtual Private Network (VPN) realm

*This block is essentially materialised by the protocols implementing the Federation for Epidemic Surges Protection (*EpiProtect*) VPN, linking the institutions entrusted to manage epidemic tracing, and associated institutions.*

The VPN is supposed to interconnect all nodes of the architecture, through Edge and Core PriLock Information Switches: Edge PriLock Secure Clouds (PSC); Core PriLock Secure Clouds (PSC); PriLock Complex Event Processing Engine (PCEPE); PriLock Data Vault (PDV); any PriLock Entrusted Authorities (*PEA*) not co-located in one of the facilities listed above; and privileged PriLock-Associated Entities (*ASE*) needing secure access.

3.2.5 Edge realm: associated entities

PriLock-Associated Entities (*ASE*) facilities (existing).
PriLock is destined to fulfill several societal objectives. As such, it is natural that one of the needs is the secure information export to, or import from, external entities needing to work on it. The particular information may or not have privacy criticality.

In consequence, PAE that only need to receive or send non-critical information will do so by standard information transfer mechanisms. PAE that need to receive or send critical information as well MUST do so via mechanisms provided through the Federation for Epidemic Surges Protection (*EpiProtect*) VPN.

This will be implemented by means of a protocol to be established between the *EpiProtect* and the relevant PAE, and materialised through an Edge PriLock Information Switch (Edge PIS) connected to the VPN, similar to those used in the Telco Providers edge.

Any significant amount of critical information leaving the PDV to *ASE* (PriLock-Associated Entities), e.g., for research purposes (such as statistical collection and epidemics modelling), should provide strong guarantees of anonymity and generic protection of any PII (that has in the meantime not been made non-private, e.g., according to the laws of some countries with regard to notifiable diseases). N.B.- The words of caution made about in-core workflows under more sophisticated operations are echoed here by majority of reason, for externalisation of information to associated entities or the public. Before allowing, in further versions of PriLock, more aggressive release of information without raising the risk, and additionally to what was suggested for the improvement of the security of the in-core workflows, further research is suggested on the investigation and verification of algorithms allowing privacy-preserving information disclosure, for example leveraging s.o.t.a. on k-anonymity [38] and its successive refinments [32, 30], or differential privacy [14, 15, 16].

3.2.6 Core realm

The Core realm consists of facilities containing the storage and computing capacity to handle the PriLock operation. To be instrumented in facilities of the PriLock Entrusted Authorities (*PEA*), as extensions of existing installations, or created anew.

Core PriLock Information Switches (Core PIS).
Containing some core services and the connection to the VPN).

Core PriLock Secure Clouds (PSC).
In the *PEA* Data Centers, containing private storage and compute clouds supporting other components, see below). The Core PriLock Secure Clouds (PSC) are a compound of clouds in the core facilities of PriLock (*PEA*). They offer the decentralised basis for running distributed protocols implementing the PriLock Complex Event Processing Engine in a distributed and parallel instantiation, and the PriLock Data Vault in a resilient (fault and intrusion tolerant) way. Both are described below.

PriLock Complex Event Processing Engine (PCEPE).
PCEPE is the engine where computations are massively run, in principle implemented in one or more Core PriLock Secure Clouds (PSC), in *PEA* Data Centers.

In PCEPE, collected events (paging information) are processed and tracing information is extracted and stored in data vault. PCEPE has to operate on streams of information, in near real-time and, above all, has to be implemented as trusted computing service. PCEPE is designed as a streaming system as it has to run continuous queries on constantly arriving input data, in order, to capture the ever changing locations of potential subjects. On the contrary, batch processing would require storing of large volume of raw data and would be inefficient for this purpose. PCEPE architecture has to be dependable, and at the same time, scalable. Such complex processing engines already exist as a research prototypes, i.e. Massif project [21, 22, 8], but also reached maturity level where they have been adopted by industry and deployed in production, including BeepBeep-3 [5], Apache Flink and Storm [3], SQLstream [36].

PriLock Data Vault (PDV).
PDV is the main data repository. Though logically centralised, the PriLock Data Vault (PDV) construction is NOT physically centralised. It is distributed, as depicted in Figure 3 and as we explain below, amongst several *PEA* entity nodes, an independence that provides decentralisation of operation and resilience to faults and attacks. PDV is essentially a data store, in principle key-value in its nucleous, implemented by one or several core private storage clouds where pre-processed and post-processed data are stored. To reap performance benefits, the compute clouds needed to perform the PriLock workflows are co-located in the same *PEA* facilties, as shown in the figure. The highly secure workflows PriLock is destined to run, are coordinated from distributed protocols running on the VPN, in the several core PriLock information switches (Core PIS) which, recalling Figure 1, isolate and connect the PriLock components running in several facilities.

The PriLock VPN and Data Vault compound represented in Figure 3 is a crucial building block which builds on a large body of knowledge on fault and intrusion tolerance and resilience (e.g., Byzantine fault-tolerance, cloud-of-clouds tech., multiparty cryptography, erasure coding, etc.). One of the central fears and a threat to be reckoned with is the execution of sensitive operations by a single or minority groups of entities. PriLock addresses these possible threat vectors by requiring consensus for all critical operations by a quorum of independent entrusted entities. At the level of machines invoking services at other machines, classical solutions, such as Byzantine fault tolerant state-machine replication protocols (e.g., PBFT [10], MinBFT [39], CheapBFT [27], but also variants deployed in modern blockchains [2, 1, 23, 24, 34, 20, 28]) are readily available.

We detail the security and dependability aspects of the PriLock VPN and Data Vault compound represented in Figure 3, in the next section.

3.2.7 Security and dependability aspects

Security and dependability of Core subsystems: Policy aspects.
Queries, and direct reads and writes can be made on PDV under incremental authentication and

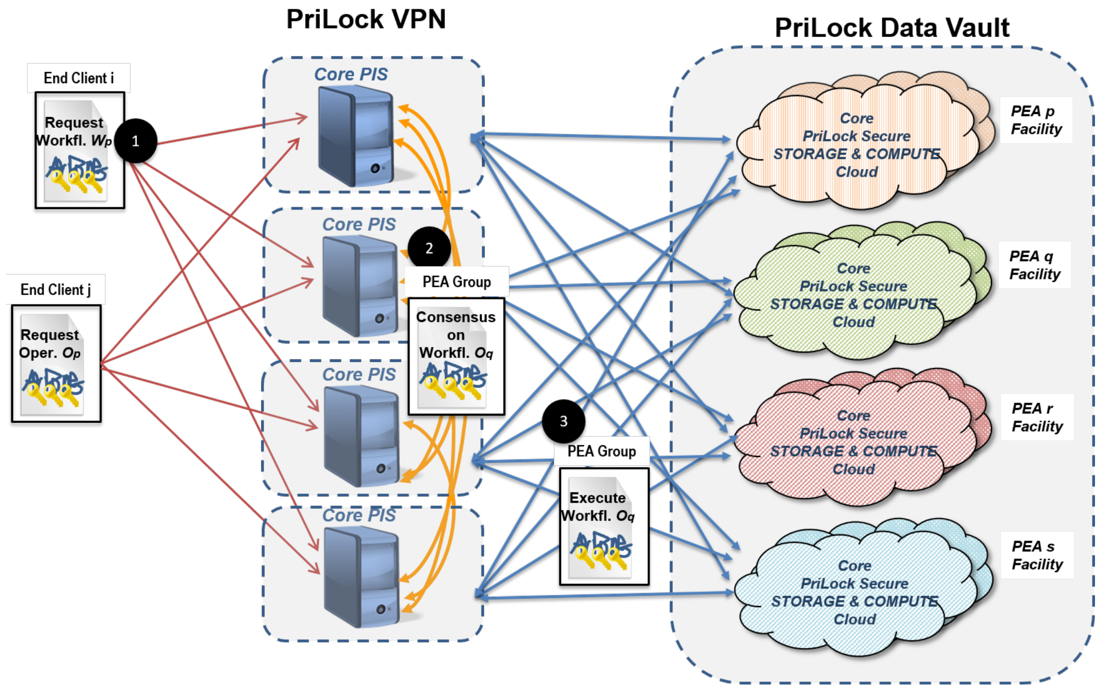

Figure 3: PriLock Data Vault: Consensual triggering of operations

authorisation policies established by policy makers, issued by quorums of the *PEA* entities and implemented by the technologies underlying PDV.

As explained elsewhere, PriLock follows generically a 2q-eyes access control policy: it is necessary that q entities amongst the n entrusted ones, vet any transaction that modifies or extracts information from the Vault. The size of quorum q may vary with the class of operation (also discussed elsewhere).

Generically, depending on the operation, q corresponds for example to x+1 minimum number of unblocking shares of an (x+1, n) multiparty crypto operation, such as a threshold signature, or the recovery of the (x+1,n) shared key protecting PDRs in edge clouds, or other processed records in the core data vault clouds. The quorum q may also correspond to some f+1-fault tolerant quorum of entities needed to secure a majority vote on operations that relinquish, or allow modification of, information in the PDV.

The workflow to gather the necessary authorisations should be apparent to the entities involved. For example, when requested by one of the entities involved in the activities of the Epidemic Tracing and Prediction Federation, it only goes ahead after being authorised by enough other entrusted entities. For this to be done without large impact on the efficiency, decision and operation processes should be streamlined and based on IT-supported workflows (e.g., through some form of ERP systems workflow support).

In the example of Figure 3, such authorised requests for single operations or workflows (1) (gathering the necessary number and qualities of signatures) are arriving at the PriLock interface, broadcast to all core PIS. The BFT protocols in the PIS run in order to reach a consensus (2). Each PIS resides in a facility that is managed by and represents an independent stakeholder of the system, as we have discussed before. That is, even in the presence of f faulty players or attackers, in the end there is at least a majority number of correct players agreeing on what the workflow should be, and thus ending-up deciding to execute the correct workflow (3).

Now, the workflow, as depicted in the Figure, combines access to the data at rest in the storage clouds, with the computational elements in the compute clouds, for example, the PCEPE. The workflow is triggered by the BFT protocols in the PIS, ensuring that it is correctly implemented, and maintaining the security properties desired of the Vault data, namely privacy.

Again, no data can be extracted except in a consensual manner.

Security and dependability of Core subsystems: Technology aspects.
In order to prevent the risks to security and dependability (most especially abuses against privacy), we have just seen that the policies behind management and access control of the PriLock Data Vault (PDV) are not single point. We have explained that *PEA*, the group of entities entrusted to manage it, must be formed following the checks-and-balances principles.

It is important to explain the workings and structure of the PriLock Data Vault (PDV) construction with a bit more detail, which we do in Figure 4, as that storage repository assumes an enormous criticality in the operation of PriLock, since it holds primarily PII.

Again, principles of distributed fault and intrusion tolerance (a.k.a. Byzantine fault tolerance, BFT) are followed in the implementation of the mechanisms controlling the access to the repository, and the repository units implementing the latter. This middleware transforms the logical centralisation in physical decentralisation, over a set of distributed nodes. For example, secret sharing [35] prevents unilateral reconstruction of confidential information (e.g., by malicious insiders), erasure coding [26] provides the same property for data integrity, preventing unilateral damage, and deploying such encoded data over mutually distrusting clouds [6, 7] extends these properties to less trustworthy infrastructures (such as public clouds or, as is the case for the PriLock Data Vault, private clouds in the *PEA* premises to protect this highly-sensitive data at the highest degree possible).

The design is based on the works of [6, 7]. As Figure 4 shows, all starts with a register or file access request, read or write. Connecting to Figure 3, this request would be part of the workflow execution (3), PIS acting as clients. Let us imagine a write request. A key is generated on the fly (1), the file encrypted (2). Then it is split in several pieces by erasure coding (4 in the example). Key shares are calculated for the key (4) (4 in the example). Then, both the file pieces and the key shares are scattered over several clouds, in several sites. Reading reverses these steps.

Concisely, this design leverages the natural redundancy and possibility of scattering of PDV over several storage clouds in the *PEA* elements. This has the virtuous effect of complementing the protection, by reducing the threat surface (the exposure to attacks, e.g. but not only, on privacy) presented both to external attackers, and to insiders from within each *PEA* member entity. PDV access through the VPN will thus be controlled by protocols running in the several core PIS of the *PEA*, establishing consensus or matching thresholds for the operations.

These implementations should be transparent to the users, to preserve the benefits of logical centralisation, and integrate well with the above-mentioned workflows. As sophisticated as it may be, there is in fact technology emerging from research over the past few years, available with a high TRL (technology readiness level) to make this objective a feasible one. Since we foresee that ALL operations are systematically attested and certified, the integration of BFT protocols is also an easy means to effect indelible logging and/or blockchain supported ledgers (many, if not most of the blockchains of late are implemented based on BFT).

Security and dependability of Core subsystems: Data Protection Regulation aspects.
We foresee that the operations on the PriLock Data Vault (PDV) secure the principles of data minimization and storage limitation followed by data protection authorities and the GDPR in general. After post-processing of data extracted, all redundant data must be immediately disposed of, and we are assuming that the remaining data is the one meaningful for the classical operation (i.e., without PriLock) of the state services such as the NHS, for example, the identification of infected, or suspected infected subjects.

N.B.- The current baseline architecture minimizes the threat plane and achieves high resilience, under the premise that in this first version, the most pressing requirements R1-R4 are fully met in a highly secure way. In essence, extracting efficiently and in near real-time, information that would end up in standard systems, e.g., the NHS, albeit in a much more painful, slow and incomplete way. For example, the identification of infected, or suspected infected subjects.

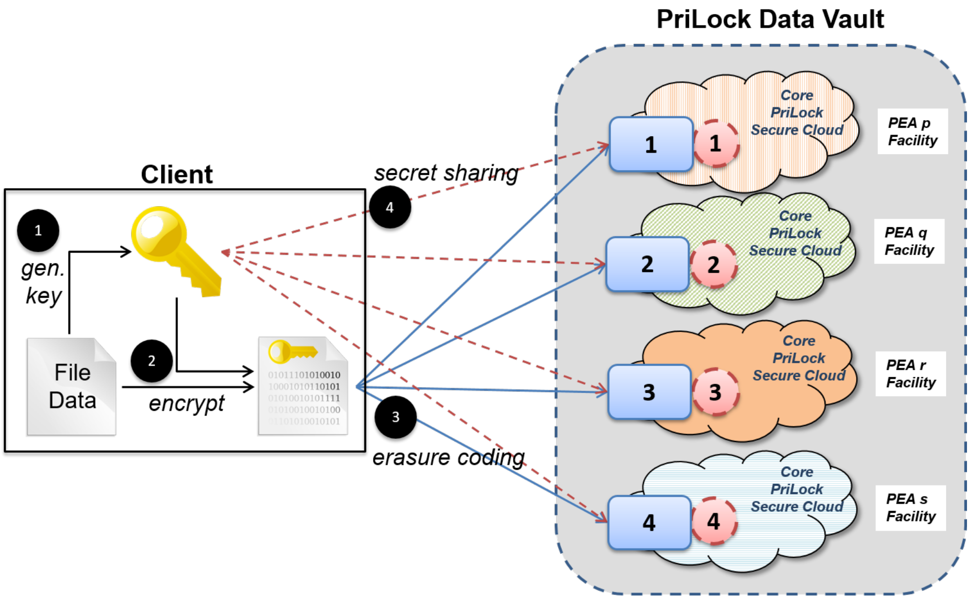

Figure 4: Security and dependability of PriLock Data Vault storage

Other richer (and useful) services — e.g., with regard to other requirements, which we certainly endorse — possible over the PDV information, should follow the precautionary principle of general law, as well as the purpose limitation principle of GDPR. S.o.t.a. research has been showing that preventing re-identification (de-anonymisation) is a quite difficult task, especially when one has access to additional spatial-temporal events about the subjects, acquired by OSINT (open-systems intelligence) or other means [12, 13, 25]. As such, extreme care should be taken in the handling of that information in a more risk prone way.

With regard to maintaining the resilience level of the in-core workflows under more sophisticated operations, further research is suggested on the investigation and verification of algorithms allowing distributed privacy-preserving workflows over the VPN, for example leveraging s.o.t.a. partially homomorphic encryption and secure multiparty computation.

3.3 Information flow

Information flow will depend on the system state and the operation mode invoked.

System states: At any given moment, the system is in one of the following states:

1. ***Passive*** - the system is working as a pruning passive listener, and keeps a minimal amount of information, in the form of PDRs, which are encrypted and written continuously to/from the Edge PriLock Secure Clouds (PSC) (in Telco Provider cellular Controlling Data Centers). However, the PDRs are constantly pruned: only a recent history of PDRs is there, but inaccessible. The Clouds are locked to operations from the VPN (and reading from the Provider is technically infeasible). PriLock Data Vault (PDV) is either empty, or locked for reading or writing, depending on the implementation approach. The unlocking of both the vault and the secure clouds is a highly-critical operation, see below.

2. ***Alert*** - the system starts to operate to face a potential epidemic, and the information flow to and through the core starts. The Edge PriLock Secure Clouds (PSC) (in Telco Provider Cellular Controlling Data Centers) and the PriLock Data Vault (PDV) are unlocked. The unlocking of both the vault and the secure clouds is a highly-critical operation, see below. In this state, the system core may store raw, pre-processed and post-processed PDRs, always in encrypted form, through the period of duration of the alert.

Operation modes: There are several operation modes of different criticality, defining different authorisation (access control clearance) criteria for the different entities. The modes are impacted, amongst other factors, by the criticality of information with regard to privacy. Critical information is any piece of data that has at least one PII-critical record):

- ***Lock/unlock*** – operations which materialise the change of state from Passive to Alert, or vice-versa, namely and respectively, unlocking or locking the core Vault and the edge Secure Clouds, and starting other services such as the CEP Engine.
- ***Strict push*** – operations are write-only, no read possible.
- ***Blind analysis*** – operations can read from encrypted data (e.g., encrypted searches), and will be supplied the needed metadata.
- ***Blind processing*** – operations can read/write from/to encrypted data (e.g., encrypted searches, partially homomorphic update actions), and will be supplied the needed metadata.
- ***Full processing*** – operations can read/write from/to cleartext data (e.g., record searches, update and record creation actions), and will be supplied needed metadata, such as decryption/encryption keys.

Whenever possible, operations on cleartext data should be done under protection of Trusted Execution Environments (TEE, such as Intel SGX, or ARM TrustZone). Information containing critical data should be encrypted before written into a PriLock repository (e.g., the PriLock Data Vault (PDV)).

Notation:

e_p^i - event of ordinal i, happening at p.

$t_x(a)$ - real time instant related to x, for example $x = 0$: start, or

$x = in$ - entry, etc., happening at participant a.

δt_x - real time interval related to x.

T_x - predefined time instant or interval, related to x. For example a message delay, or a timestamp of a real time instant, or other system constant or variable.

T_x^p - idem, happening at participant p.

Edge realm:

Proximity Detail Record (PDR) are the source records containing raw relative proximity data of phones w.r.t. a base station BS_i. They are issued by each base station every minute p of the clock, and thus synchronised at all providers. They are organised in sets of tuples of the following format:

$$\mathtt{PDR}_k^p\left(\mathtt{code}(BS_i),\ \mathtt{Phone}_k(nr, imei),\ \mathtt{ProxVector}_k(BS_i),\ T_{pdr}^p\right)$$

$$\mathtt{PDR}^p = \{\mathtt{PDR}_1^p, \cdots, \mathtt{PDR}_n^p\}$$

The set $\mathtt{PDR}^p$ is then encrypted.

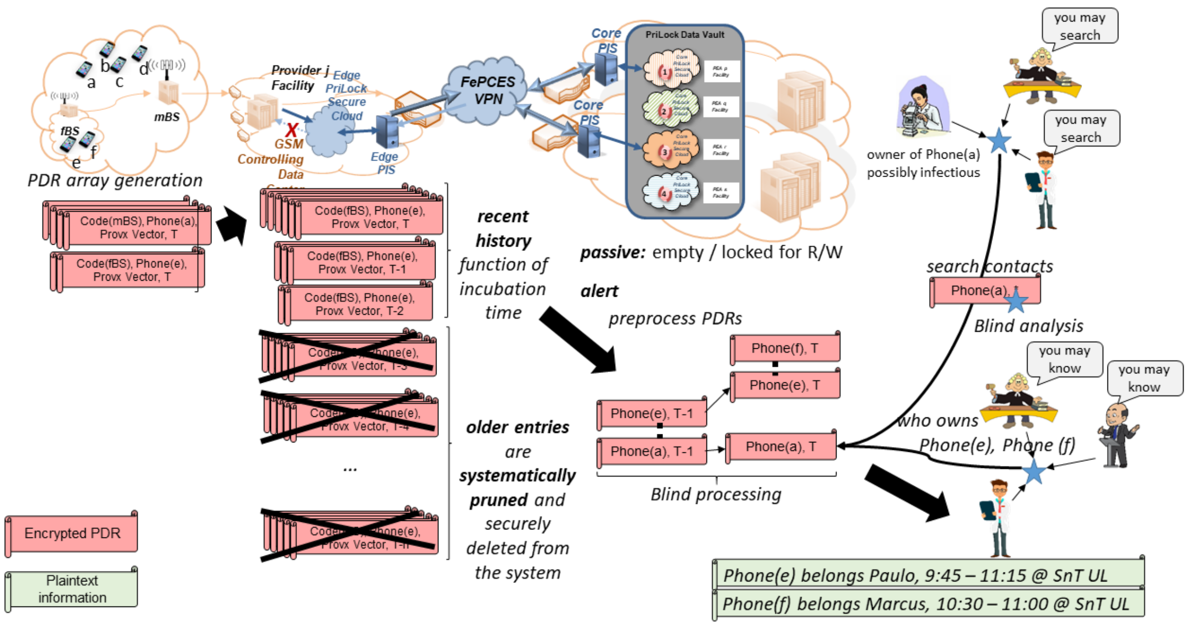

Figure 5: Information flow through the PriLock architecture. The recent history of encrypted PDRs is collected in the Edge PriLock secure cloud infrastructure and, after the system is alerted, blindly preprocessed. Given authority through the federation, PDR contacts of positive tested individuals can be searched through blind analysis. Once records of possibly infected individuals are found and extracted, their identity can be selectively released (e.g., to NHS), given consensual approval through the *EpiProtect* members.

PDRs from Telco Provider Cellular network cells, macrocells and picocells (and PriLock femtocells) are continuously collected by each Provider, encrypted with an asymmetric public key made available by the PriLock Entrusted Authorities (*PEA*) to the Providers (or each provider for fault independence), and then stored in push mode (unilateral write-only mode), in the Edge PriLock Secure Cloud (PSC) (in Telco Provider Cellular Controlling Data Centers).

The timestamp of creation of the PDR, T^p_{pdr} is also annexed as cleartext metadata, for pruning. From now on, this data stays at rest and can only be accessed from the Federation for Epidemic Surges Protection (*EpiProtect*) VPN, through the Edge PriLock Information Switches (*Edge PIS*) (containing the edge services and connection to the VPN). A time-to-live parameter PDRttl is set to a value defined by the NHS experts. The rationale is "how long back should tracing go, when a first infection notice is known?" (this could be "in the country" or, experience advises, "in the world"). This time will be a function of the disease incubation time, T_{incub}. A value like at least twice or thrice the incubation time gives an idea. The PIS controls the time-to-live parameter of each PDR record, from its T_{pdr} and everyday erases, through secure delete, the PDRs whose life has expired.

VPN realm: The flow of *critical information* should only be made through the Federation for Epidemic Surges Protection (*EpiProtect*) VPN, which runs amongst the Edge and Core PIS, offering protocols protecting security and dependability of communication.

Core realm: Most of the time (hopefully), the system is in Passive state. As such, it is almost empty of information, as seen above, and both the vault and the secure clouds are locked.

So, now let us analyse the information flow when the system goes to Alert state, after being unlocked by a highly-critical operation, see below. In this state, the system core starts analysing and processing essentially three kinds of records:

- *Raw PDRs* – start coming from all Providers, during the Alert interval, as necessary for the workflows.
- *Pre-processed PDRs* – Results of analysis of raw PDRs, destined to improve the precision of determination of the PDR parameters, as well as finding and scoring simple proximity suspicions between pairs of phones in the space-time, across different providers.
- *Post-processed PDRs* – Results of analysis of pre-processed and/or raw PDRs, destined to create insights about infection propagation and chains thereof.

Pre-processing: The operations below are triggered in consequence of a certified request from the *PEA*, to find out about one or more phone(s) of interest for holders being (or suspected as being) either infected or infectious (checked with the NHS). Information given is $\texttt{Phone}_v(nr, imei)$ and estimated earliest infection instant $\texttt{Phone}_v(Tinf_{min})$, when it is believed that holder was potentially contaminated.

Finding suspicions: We start by finding for a phone of interest (and repeated for all phones of interest). This operation can happen at any time during the Alert state, so we should narrow the search in function of the incubation time T_{incub} (we consider this number is calculated as the worst case (longer) and already including the margin of error).

Note that we wish to know both who could have infected the holder of v, and who v could have been infecting after being infected. Given a phone of interest $\texttt{Phone}_v(nr, imei)$, this means finding all the $\texttt{PDR}^p = \{\texttt{PDR}^p_1, \cdots, \texttt{PDR}^p_n\}$ sets where v exists, and such that for all p, $T^p_{pdr} \geq Tinf_{min} - T_{incub}$.

So, in a time series $p_1, \cdots, p_k$, we have a varying list of phones that have appeared near v, during different parts of the time series. Consider P the set of all these phones.

Now, for each pair of phones (v, u), where $u \in P$, we find all occurrences that situate both in some same space-time region (one or several subseries $p_i, \cdots, p_j$ within the $p_1, \cdots, p_k$ interval).

Inside that group of registers for (v, u), we refine the precision of the notion of distance (remember we may have events from mBS, pBS, fBS) between the pair, as well as the notion of duration (remember that there may be noise, and/or both phones e.g. may wonder at a short distance, but between pBS and/or fBS e.g. in a mall, in an interval of minutes).

Now consider a threshold, to be defined by NHS scientists and technicians, for the minimum spatio-temporal contact values to raise a potential contamination suspicion (boolean PC_{susp}), of $Prox_{min}$ and Dur_{min}.

We analyse the data, and in result, identify hits of a condition:
$PC_{susp}(v, u) = True \texttt{ if } (Prox(v, u) \leq Prox_{min}) \wedge (Dur(v, u) \geq Dur_{min})$

After this analysis, we obtain a list of "suspected" potential contamination pairs. Now, this list is important for the *PEA* entities as a quick though coarse output in reaction to some event. However, it would be necessary to continue and refine those suspicions, according to a scale of risk of infection.

Scoring suspicions: We now continue refining the suspicions. We need to define the confidence we put in each suspicion, $PC_{scor}(v, u)$. Note that there may be input from several suspicion events, most possibly within a paging cell (mBS, pBS, fBS). For simplicity, and without loss of generality, let us call the target of our scoring effort, a space-time region R_b, that is, a certain interval of time in a certain limited perimeter of space.

This is a multivariable calculation, where heuristics also find a place, in more refined future versions, especially as the infection mechanisms of the disease start to be better known. It must be remembered that PriLock is a generic system, for any epidemic infection to come, possibly unknown. To give it a start, we define a simple enough function for now:

$$PC_{scor}(v,u,R_b) = f(R_b,\ Prox_{avg}(v,u),\ Dur_{tot}(v,u),\ precision(Prox),\\ precision(Dur),\ density(R_b),\ severity(R_b))$$

And we create corresponding tuples with the scores and the function terms, which are stored:

$$PC_{scor}(v,u,R_b)\ (PC_{scor}, R_b,\ Prox_{avg}(v,u),\ Dur_{tot}(v,u),\\ precision(Prox),\ precision(Dur),\ density(R_b),\ severity(R_b))$$

R_b is described by the envelope interval of time of the evaluation and the envelope of the space area considered (i.e. paging cells). $Prox_{avg}(v,u)$, $Dur_{tot}(v,u)$, account for the periods of at least Dur_{min} where (v,u) have been at or nearer than $Prox_{min}$, summing-up and integrating that time ($Dur_{tot}(v,u)$), and also considering how actually close they were on average (even below the min) ($Prox_{avg}(v,u)$). That is, if there were 4-5 of periods, e.g., walking in a mall separated by short intervals, and they were even closer than the min, the whole summed-up duration and the real distance should be reflected in the score. Conversely, if two subjects were located as being not too near under a same fBS, but they were e.g., sitting in a restaurant for over a couple of hours, that should as well be reflected in the score. The parameters $precision(Prox)$, $precision(Dur)$, are heuristic contact evaluation factors accounting for the coverage of the translation of *digital proximity to actual contact*.

Remember that PriLock assumes a default baseline measurement approach based on the cellular apparatus, for inclusion, fairness and completeness. As said before, it welcomes integration of other approaches on a voluntary basis, which may complement information in specific situations and areas, e.g., those implemented by GPS, Bluetooth, Wifi or other. However, given recent discussions[18] care must be taken to make that integration in a way taking into account the non-functional objectives (R7-R10), in particular digital sovereignty.

Parameter $precision(Prox)$, accounts for a scale of quality of the method of measurement of distance (mBS, pBS, fBS, BLE, Wifi, GPS, etc.).

Parameter $precision(Dur)$, accounts for a scale of quality of the measurement of the real infecting contact. It may assume a default value for lack of more information, but may take into account specific additional information when the algorithm is improved, such as speed of trajectory of v, u in R_s, outside/inside, vehicle, stopped (e.g. sleeping), short (at a room), etc.

Parameter $density(R_b)$ is specific of the space-time region and accounts for the average density of phones (number over useful range) registered in it during the interval in appreciation. It may be a provider-supplied parameter, or can be obtained from the PDR data, but can assume a default value for a start. Parameter $severity(R_b)$ is again a heuristic parameter that may assume a default value for lack of more information, but may take into account specific additional information when the algorithm is improved, e.g., the social role of R_s area: street, theatre, mall, restaurant, hospital, retirement home, etc.).

Whatever the function, PC_{scor} will be discretised to assume a range of discrete values, for practical utilisation by the *PEA*. Let us assume a range of 1-4, where highest means highest risk of the potential contamination (this is conveyed quite well by the function terms, since risk magnitude = probability * impact): 1- Low; 2- Moderate; 3- High; 4- Very High.

The mission of PriLock in this case is to evaluate the risk of contamination between a pair of phone holders as precisely as possible, also with input from *PEA*, e.g., w.r.t. to the heuristic

[18] https://www.letemps.ch/economie/singapour-tracage-app-degenere-surveillance-masse

parameters. At this point, the diagnostic for a set of (v, u) pairs is done, both in terms of boolean early warning suspicions, and a grading of those suspicions. The score gives an opportunity for selective handling. Several differentiated actions can be triggered as a function of the score, to be defined by the NHS/*PEA*.

Post-processing: There will be several avenues for post-processing. Upon analysis of the pre-processed data, the *PEA* entities will decide for several courses of action w.r.t. each pair, depending on the above risk classes. These may imply further analysis of the information by PriLock.

An obvious C.o.A. (course of action) for high enough PC scores of given pairs (as considered by the NHS), besides any other actions, is to complete the potential contamination findings related to this pair, by repeating the pre-processing steps for the other phones.

Another obvious C.o.A., as high or very high PC score pairs turn into infection-positive, besides any other actions, are: find the potential infection chain (e.g., ordered chains of holders of phone pairs upstream and downstream some target phones pair); find potential hotspots or infection trajectories (e.g., resp., a very packed restaurant in fashion, or a bus with one or more infected persons, riding from a high-level infection area to a remote yet uninfected town).

We assume again that these operations below are triggered in consequence of a certified request from the *PEA*, to find out about potential infection chains or potential hotspots or infection trajectories, related to one or more phone(s) of interest for holders phones having a sufficiently high potential contamination score (checked with the NHS).

Complete potential contamination findings: Given v, u pairs with high enough PC scores, we should re-invoke the pre-processing steps as above for each u, and find all possible PC_{susp} and then PC_{scor} with phones other than v.

Finding the potential infection chain: In time, the majority of people part of the contacts found in this batch should have been tested and/or signalled as sick by the NHS. We assume earliest infection dates $Tinf_{min}(v)$ were calculated for all v.

We go to the repository of pre-processed $PC_{scor}(v, u, R_b)$ registers and create a database containing a new set of registers, containing only those where v and u are both known contaminated at current time, and add the respective earliest infection times. We add as well the coordinates of space-time region R_b where the contact was identified, as well as the median of the contact interval:

$$PC_{cont}(v,\ u,\ R_b)\,(v,\ u,\ R_b,\ coord(R_b),\ median(\Delta T_{contact}),\ Tinf_{min}(v),\ Tinf_{min}(u))$$

Note that these PC_{cont} registers are annotated versions of the $PC_{scor}(v, u, R_b)$ registers, they tell the whole history since recorded, and $Tinf_{min}()$ is added now. So they may refer to contact space-time points where neither or one of v or u had yet been identified contaminated i.e., it could be that $\Delta T_{contact} > Tinf_{min}()$. So, at this point, just by looking at one register, we do not know whether v infected u or vice-versa. To find the chain, we have to be able to trace the potential causality in the real-time domain, between the contact events PC_{cont}.

The problem can be reduced to a potential causality determination problem, leading to a partially ordered directed acyclic graph (DAG), from which many of the insights desired can be withdrawn. We will rely on a generalisation of Lamport's 'happened before' theory for logical channels, to models allowing the determination of potential causality in the temporal domain for any channels. We consider the combined analysis of the time-like separation of contamination events, with the minimum and maximum incubation times as granularity parameters, and the space-like separation of related contact points between two phone holders.

Finding potential hotspots or infection trajectories: Note that this will be an evolving process, which will be updated as more phones from holders tested positive are inserted. This way we can follow, and at a certain points predict, the trajectories and evolution of the epidemic. For example, from the DAG one can create a georeferenced projection of infection charts: density, propagation trajectories, etc. For finding hotspots, we should search the repository of positive pairs and do a density map according to the coordinates of the respective space-time regions R_b. As the epidemic evolves, these tools will allow the NHS/PEA to make decisions quickly, effectively and as accurately and minimally disturbing as possible.

3.4 Security, Dependability and Resilience analysis

Security of information treatment from the base stations down to the core servers is the responsibility of the infrastructure holders. The incumbents should collectively ensure:

- Storage of PDRs at the Edge Clouds with multiparty encryption technology.
- Minimisation of storage of PDRs at the Edge Clouds, by continued periodical deletion.
- Lock of the Edge Clouds for Provider read access.
- Full lock of the Edge Clouds during passive state.
- Fault and intrusion tolerance of the Core Clouds, by:
  - (i) enforcing $k_i + 1$ entities to contribute to authorise and/or certify in ledger any critical operation;
  - (ii) enforcing $k_j + 1$ shares to reconstruct any decryption key;
  - (iii) enforcing $f + 1$ diverse nodes to reach consensus on operations or sets thereof on the Clouds;
  - (iv) considering quorums of diverse software/hardware replicas to reach availability in the face of faults or attacks
  - (v) enforcing highly secure and robust communication on the VPN.
- Minimisation of operations in the clear on critical data, leveraging:
  - (i) utilisation of searchable encryption technology to the extent possible;
  - (ii) minimisation of cleartext manipulation risk by leveraging TEEs in the compute clouds.
- Minimisation of critical data storage in the Core Clouds, namely Vault, by:
  - (i) eliminating data as it becomes not needed after being processed, during the Alert state
  - (ii) performing secure delete of all data, as permitted by regulations, as soon as the system enters Passive state.

3.5 Interaction with other societal systems

PriLock is destined to fulfill several societal objectives and as such close interaction is expected with these entities. In particular, PriLock needs to be configured with parameters to be defined by NHS scientists and technicians, and refined throughout its operation. For example, when searching for suspicious encounters (see finding suspicions on page 17), the incubation time needs to be adjusted to the knowledge epidemiologists have gathered about the current infection.

Epidemiology experts are also expected to benefit from post-processed information supplied by PriLock, especially during the active stages of infections and epidemics. However, even though PriLock would rely on established procedures and regulatory frameworks (approval from ethics committees, etc.) to grant access to this information on an urgent need to know basis, by enabling authorized entities to extract sanitized statistical information and pseudomized data sets, we believe further research is required to ensure the protection of citizens rights, in particular privacy, for less urgent needs.

3.6 Cross-border interoperability

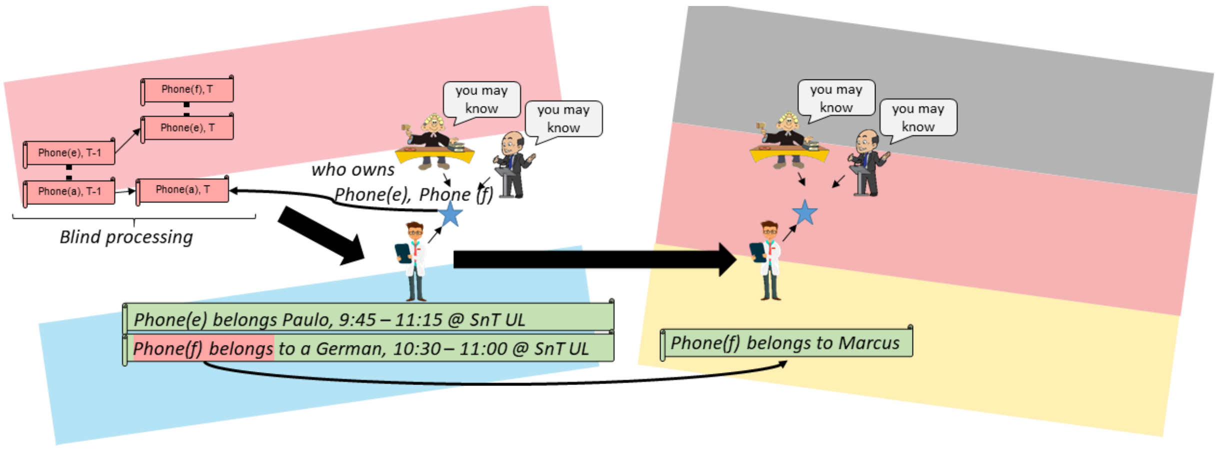

Figure 6: Cross-border infection chain tracing through PriLock

One aspect of interaction we wish to highlight here, is the interoperability with systems applied in other countries. PriLock is by design a single nation system in the sense that through PriLock citizens entrust their PII data to the federation of entrusted legal authorities, either elected, or appointed by an elected government, and which form the *EpiProtect*. As such, federations or members of other countries have in principle no right over these citizens' PII data.

However, it is of course essential to be able to follow infection chains across countries and to alarm the respective authorities about the possibility of an infection, or worse a new outbreak.

Much like roaming supports foreigners to obtain access to the mobile communication network, PriLock is trivially cross-border interoperable by not revealing the identity of foreigners to another countries *EpiProtect*. Instead, the final step of reidentifying the person behind the PDRs it creates is reserved for the country this person lives in. More specifically, PDRs ultimately can reveal the space-time coordinates where infections may have happened and the contacts this person had, including the country she lives in, but to reidentify this person, authority of the *EpiProtect* of this person's country will be needed. Figure 6 illustrates this point.

Barring the technical details, the existing good collaboration between national health institutes in Europe and world wide, already suffices to continue tracing infection chains across borders by a simple exchange of those found encrypted phone-identifying tokens, which only the *EpiProtect* of the respective country will be able to decrypt to reveal the person behind. Although much easier with PriLock instances on both sides of the border, which continuously track the infected and his contacts through PDRs, the possibility of the home country's *EpiProtect* to learn about the phone and its owner continues to work with fundamentally other tracing systems.

3.7 Acknowledgments

We could not have created this preliminary design specification without the help and contributions of a number of people. The fact of them being experts at different levels of the architecture and of the hardware/software stacks on which PriLock is built, substantiates our words in the beginning, that this a complex distributed critical information systems problem which needs diverse skills such as distributed algorithms, fault and intrusion tolerance, networking and cloud technology, cryptography, amongst others, not forgetting the contribution of the medical fields to establish requirements and needs. We would particularly like to express our special thanks to Rui Aguiar, Alysson Bessani, Adam Lackorzynski, and Bernardo Rodrigues. Thanks for helping out when and where we had doubts or struggled.

References

[1] Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Alexander Spiegelman. “Solida: A blockchain protocol based on reconfigurable byzantine consensus”. In: *arXiv* (2016).

[2] Elli Androulaki et al. “Hyperledger fabric: a distributed operating system for permissioned blockchains”. In: *EuroSys conference*. 2018.

[3] *Apache Storm*. `http://storm.apache.org/`.

[4] Gennaro Avitabile, Vincenzo Botta, Vincenzo Iovino, and Ivan Visconti. *Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System*. Cryptology ePrint Archive, Report 2020/493. `https://eprint.iacr.org/2020/493`. 2020.

[5] *BeepBeep-3*. `https://liflab.github.io/beepbeep-3/`.

[6] Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando André, and Paulo Sousa. “DepSky: Dependable and Secure Storage in a Cloud-of-Clouds”. In: *ACM Trans. Storage* 9.4 (Nov. 2013).

[7] Alysson Bessani, Ricardo Mendes, Tiago Oliveira, Nuno Neves, Miguel Correia, Marcelo Pasin, and Paulo Verissimo. “SCFS: A Shared Cloud-Backed File System”. In: *Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference*. USENIX ATC’14. Philadelphia, PA: USENIX Association, 2014.

[8] Alysson Bessani, Joao Sousa, and Eduardo Alchieri. *State Machine Replication for the Masses with BFT-SMART*. Tech. rep. TR-2013-07. http://hdl.handle.net/10451/14170. University of Lisbon, DI-FCUL, Nov. 2013.

[9] Ran Canetti, Ari Trachtenberg, and Mayank Varia. *Anonymous Collocation Discovery: Harnessing Privacy to Tame the Coronavirus*. 2020. arXiv: `2003.13670 [cs.CY]`.

[10] Miguel Castro and Barbara Liskov. “Practical Byzantine Fault Tolerance”. In: *Proceedings of the Third Symposium on Operating Systems Design and Implementation*. OSDI ’99. New Orleans, Louisiana, USA: USENIX Association, 1999.

[11] Justin Chan et al. *PACT: Privacy Sensitive Protocols and Mechanisms for Mobile Contact Tracing*. 2020. arXiv: `2004.03544 [cs.CR]`.

[12] Yves-Alexandre De Montjoye, César A Hidalgo, Michel Verleysen, and Vincent D Blondel. “Unique in the crowd: The privacy bounds of human mobility”. In: *Scientific reports* 3 (2013).

[13] Yves-Alexandre De Montjoye, Laura Radaelli, Vivek Kumar Singh, et al. “Unique in the shopping mall: On the reidentifiability of credit card metadata”. In: *Science* 347.6221 (2015).

[14] Cynthia Dwork. “Differential privacy: A survey of results”. In: *International conference on theory and applications of models of computation*. Springer. 2008.

[15] Cynthia Dwork, Moni Naor, Toniann Pitassi, and Guy N Rothblum. “Differential privacy under continual observation”. In: *Proceedings of the forty-second ACM symposium on Theory of computing*. 2010.

[16] Cynthia Dwork, Moni Naor, Toniann Pitassi, Guy N Rothblum, and Sergey Yekhanin. “Pan-Private Streaming Algorithms.” In: *ICS*. 2010.

[17] Ken TD Eames and Matt J Keeling. "Contact tracing and disease control". In: *Proceedings of the Royal Society of London. Series B: Biological Sciences* 270.1533 (2003).

[18] *Edmond J. Safra Center for Ethics at Harvard University.* https://ethics.harvard.edu/files/center-for-ethics/files/roadmaptopandemicresilience_final_0.pdf.

[19] "General Data Protection Regulation". In: *Official Journal of the European Union* L119 (2016).

[20] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. "Bitcoin-ng: A scalable blockchain protocol". In: *NSDI*. 2016.

[21] Miguel Garcia, Nuno Ferreira Neves, and Alysson Bessani. "An intrusion-tolerant firewall design for protecting SIEM systems". In: *Workshop on Systems Resilience in conjunction with the Conference on Dependable Systems and Networks*. June 2013.

[22] Miguel Garcia, Nuno Ferreira Neves, and Alysson Bessani. "SieveQ: A Layered BFT Protection System for Critical Services". In: *IEEE Transactions on Dependable and Secure Computing* 15.3 (June 2018).

[23] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. "Algorand: Scaling byzantine agreements for cryptocurrencies". In: *SOSP*. 2017.

[24] Guy Golan Gueta et al. "SBFT: a scalable and decentralized trust infrastructure". In: *IEEE/IFIP DSN*. 2019.

[25] Melissa Gymrek, Amy L McGuire, David Golan, Eran Halperin, and Yaniv Erlich. "Identifying personal genomes by surname inference". In: *Science* 339.6117 (2013).

[26] R. W. Hamming. "Error detecting and error correcting codes". In: *The Bell System Technical Journal* 29.2 (1950).

[27] Rüdiger Kapitza, Johannes Behl, Christian Cachin, Tobias Distler, Simon Kuhnle, Seyed Vahid Mohammadi, Wolfgang Schröder-Preikschat, and Klaus Stengel. "CheapBFT: resource-efficient byzantine fault tolerance". In: *Proceedings of the 7th ACM european conference on Computer Systems*. 2012.

[28] Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. "Enhancing bitcoin security and performance with strong consistency via collective signing". In: *Usenix Security*. 2016.

[29] Rebecca Levine. "Development of a Contact Tracing System for Ebola Virus Disease—Kambia District, Sierra Leone, January–February 2015". In: *MMWR. Morbidity and mortality weekly report* 65 (2016).

[30] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. "t-closeness: Privacy beyond k-anonymity and l-diversity". In: *2007 IEEE 23rd International Conference on Data Engineering*. IEEE. 2007.

[31] Yongkang Liu, Lin X Cai, Xuemin Shen, and Hongwei Luo. "Deploying cognitive cellular networks under dynamic resource management". In: *IEEE wireless communications* 20.2 (2013).

[32] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. "l-diversity: Privacy beyond k-anonymity". In: *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1.1 (2007).

[33] Leonie Reichert, Samuel Brack, and Björn Scheuermann. *Privacy-preserving contact tracing of covid-19 patients*. 2020.

[34] T. Rocket. "Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies". In: 2018.

[35] Adi Shamir. "How to Share a Secret". In: *Commun. ACM* 22.11 (Nov. 1979).

[36] *SQL Stream*. `https://sqlstream.com/`.

[37] Corien M Swaan, Rolf Appels, Mirjam EE Kretzschmar, and Jim E van Steenbergen. "Timeliness of contact tracing among flight passengers for influenza A/H1N1 2009". In: *BMC infectious diseases* 11.1 (2011).

[38] Latanya Sweeney. "k-anonymity: A model for protecting privacy". In: *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05 (2002).

[39] Giuliana Santos Veronese, Miguel Correia, Alysson Neves Bessani, Lau Cheuk Lung, and Paulo Verissimo. "Efficient byzantine fault-tolerance". In: *IEEE Transactions on Computers* 62.1 (2011).