ETSI GR E4P 002 V1.1.1 (2021-02)

Europe for Privacy-Preserving Pandemic Protection (E4P); Comparison of existing pandemic contact tracing systems

Disclaimer

The present document has been produced and approved by the Europe for Privacy-Preserving Pandemic Protection ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/E4P-002

Keywords
covid, eHealth, emergency services, identity, mobility, pandemic, privacy, security, smartphone

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Europe for Privacy-Preserving Pandemic Protection (E4P).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The COVID-19 pandemic has generated significant challenges for many countries and their citizens and showed that digital technologies could play an important role in addressing this and future pandemics. Various applications, services and systems for contact tracing (identification and notification of those who come in contact with a carrier) have been developed in different regions.

Despite the similar goal of automated detection of COVID-19 exposure systems as complementary solutions to manual tracing (interviews with people diagnosed with COVID-19 to track down their recent contacts), their functionality, technology, scale, required data and limitations are different and may not interoperate.

These systems are currently being deployed in different countries and many more are expected in the near future. In particular, mobile devices with their contact tracing applications can support public health authorities in controlling and containing the pandemic. In that purpose, E4P has been created to provide a technical answer to pandemic crises, not limited to COVID-19, by specifying interoperable contact tracing systems.

1 Scope

The present document provides a review of existing pandemic proximity detection methods, applications and other aspects of a pandemic contact tracing system. The similarities and differences of the various available or upcoming approaches are examined, particularly concerning but not limited to the degree of interoperability, security aspects, use of centralized or decentralized approach, use of particular proximity detection methods and technologies, support of different device platforms, epidemiological value and privacy aspects.

The review includes a grouping of various approaches into several similar types (e.g. centralized or decentralized system) and provides examples of initiatives to which the approaches apply. The present document is also neutral in terms of technologies and initiatives; however, the focus is on initiatives involving proximity sensing and networking using mobile devices, and the applications and other technical enablers which can be installed on the devices.

The present document provides a basis for the analysis of suitable requirements for a standardized solution as specified in ETSI GS E4P 003 [i.1]. It also relates to ETSI GS E4P 006 [i.2], ETSI GS E4P 007 [i.3] and ETSI GS E4P 008 [i.4].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS E4P 003: "Requirements for pandemic contact tracing systems using mobile devices".

NOTE: Not yet released at the time of publication of the present document.

[i.2] ETSI GS E4P 006: "Device-based mechanisms for pandemic contact tracing systems".

NOTE: Not yet released at the time of publication of the present document.

[i.3] ETSI GS E4P 007: "Pandemic proximity tracing systems: Interoperability framework".

NOTE: Not yet released at the time of publication of the present document.

[i.4] ETSI GS E4P 008: "Back-end mechanisms for pandemic contact tracing systems".

NOTE: Not yet released at the time of publication of the present document.

[i.5] Inter-American Development Bank: "Census of COVID-19 apps"

NOTE: Internal work document, not publicly released.

[i.6] Klinkenberg D.; Fraser C. and Heesterbeek H. (2006): "The Effectiveness of Contact Tracing in Emerging Epidemics". PLoS ONE 1(1): e12.

NOTE 1: Available at http://dx.doi.org/10.1371/journal.pone.0000012.

NOTE 2: Available at https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0000012&type=printable.

[i.7] CDC: "Key Information to Collect During a Case Interview". Centers for Disease Control and Prevention. May 21, 2020.

NOTE: Available at https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/keyinfo.html.

[i.8] CDC: "Notification of Exposure: A Contact Tracer's Guide for COVID-19". Centers for Disease Control and Prevention. August 27, 2020.

NOTE: Available at https://www.cdc.gov/coronavirus/2019-ncov/php/notification-of-exposure.html.

[i.9] Ho HJ., Zhang ZX., Huang Z., Aung AH., Lim WY., Chow A.: "Use of a Real-Time Locating System for Contact Tracing of Health Care Workers During the COVID-19 Pandemic at an Infectious Disease Center in Singapore: Validation Study". J Med Internet Res 2020; 22(5):e19437.

NOTE 1: Available at http://dx.doi.org/10.2196/19437.

NOTE 2: Available at http://www.jmir.org/2020/5/e19437/.

[i.10] Kang C., Lee J., Park Y., Huh I., Ham H., Han J.; Kim, J., Na B.: (2020): "Coronavirus Disease Exposure and Spread from Nightclubs, South Korea". Centers for Disease Control and Prevention (CDC). Emerging Infectious Diseases, 26(10), 2499-2501.

NOTE 1: Available at https://dx.doi.org/10.3201/eid2610.202573.

NOTE 2: Available at https://wwwnc.cdc.gov/eid/article/26/10/20-2573_article.

[i.11] Ardron Mitra, Peter Eckersley et alter: "Unified research on privacy-preserving contact tracing and exposure notification".

NOTE: Available at https://docs.google.com/document/d/16Kh4_Q_tmyRh0-v452wiul9oQAiTRj8AdZ5vcOJum9Y/edit.

[i.12] European Commission: "Mobile contact tracing apps in EU Member States".

NOTE: Available at https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en.

[i.13] MIT Technology Review: "Covid Tracing Tracker".

NOTE: Available at https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx__zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit#gid=1464910624.

[i.14] Wikipedia: "COVID-19 apps".

NOTE: Available at https://en.wikipedia.org/wiki/COVID-19_apps.

[i.15] Woodhams Samuel: "COVID-19 Digital Rights Tracker". TOP10VPN. March 20th, 2020.

NOTE: Available at https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/.

[i.16] Woodhams Samuel: "Covid-19 Digital Rights Tracker - Contact Tracing Apps Analysis".

NOTE: Available at https://docs.google.com/spreadsheets/d/1_BCKlMuniEhzvpQ-ha0jhdksvqdINUAUHA8J9LSr_Dc/edit#gid=0.

[i.17] Woodhams Samuel: "COVID-19 Digital Rights Tracker Supporting Data".

NOTE: Available at https://docs.google.com/spreadsheets/d/1enCBRLVCo2Dp2B0AB3tEYvLc279i5LUuoGCzoelz8aQ/edit#gid=0.

[i.18] ETSI: "E4P Terms of Reference". May 8, 2020.

NOTE: Available at https://portal.etsi.org/Portals/0/TBpages/E4P/Docs/ISG_E4P_ToR_D-G_APPROVED_20200508.pdf.

[i.19] ETSI: "New ETSI group to develop standardization framework for secure smartphone-based proximity tracing systems, helping to break COVID-19 transmission chains". Press release. Sophia Antipolis, May 12, 2020.

NOTE: Available at https://www.etsi.org/newsroom/press-releases/1768-2020-05-new-etsi-group-to-develop-standardization-framework-for-secure-smartphone-based-proximity-tracing-systems-helping-to-break-covid-19-transmission-chains.

[i.20] ETSI: "ETSI's new group on COVID-19 tracing apps interoperability moving fast: officials elected and work programme set up". Press release. Sophia Antipolis, June 11, 2020.

NOTE: Available at https://www.etsi.org/newsroom/press-releases/1780-2020-06-etsi-s-new-group-on-covid-19-tracing-apps-interoperability-moving-fast-officials-elected-and-work-programme-set-up.

[i.21] Garcia-Menendez Miguel: "ETSI Launches Industry Specification Group: Europe for Privacy-Preserving Pandemic Protection". CircleID. June 17, 2020.

NOTE: Available at http://www.circleid.com/posts/20200617-etsi-launches-europe-for-privacy-preserving-pandemic-protection/.

[i.22] EC: "Coronavirus: Commission starts testing interoperability gateway service for national contact tracing and warning apps". European Commission. Press release. September 14, 2020.

NOTE: Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1606.

[i.23] EC: "Coronavirus: EU interoperability gateway goes live, first contact tracing and warning apps linked to the system". European Commission. Press release. October 19, 2020.

NOTE: Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904.

[i.24] Vaudenay Serge: "Centralized or Decentralized? The Contact Tracing Dilemma". EPFL. May 6, 2020.

NOTE: Available at https://eprint.iacr.org/2020/531.

[i.25] Asher Saira: "TraceTogether: Singapore turns to wearable contact-tracing Covid tech". BBC News. Singapore, July 4, 2020.

NOTE: Available at https://www.bbc.com/news/technology-53146360.

[i.26] BBC News Services: "Singapore hands out coronavirus tracing devices". BBC.com. June 29, 2020.

NOTE: Available at https://www.bbc.com/news/business-53216450.

[i.27] Lausson Julien: "StopCovid: le gouvernement testera en juillet des objets connectés dédiés au traçage des contacts". Numerama.com. June 23, 2020.

NOTE: Available at: https://www.numerama.com/tech/632530-stopcovid-le-gouvernement-testera-en-juillet-des-objets-connectes-dedies-au-tracage-des-contacts.html.

[i.28] EIT Digital: "Joint efforts to develop COVID-19 contact tracing using physical tokens". Press release. May 5, 2020.

NOTE: Available at https://www.eitdigital.eu/newsroom/news/article/join-efforts-to-develop-covid-19-contact-tracing-using-physical-tokens/.

[i.29] EIT: "Anonymous COVID-19 contact tracing using physical tokens". The European Institute of Innovation & Technology. May 14, 2020.

NOTE: Available at: https://eit.europa.eu/news-events/news/anonymous-covid-19-contact-tracing-using-physical-tokens.

[i.30] The Simmel Team: "Simmel Project".

NOTE: Available at https://simmel.betrusted.io/.

[i.31] The Simmel Team: "simmel-project". GitHub.com.

NOTE: Available at https://github.com/simmel-project/frontpage.

[i.32] Palakurthi Shranav: "Project Tracer: Confidential Contact Tracing for the Masses!". Hackster.io. June 23, 2020.

NOTE: Available at: https://www.hackster.io/epicface2304/project-tracer-confidential-contact-tracing-for-the-masses-a6e2dc.

[i.33] Palakurthi Shranav: "Project Tracer". Hackaday.io. June 23, 2020.

NOTE: Available at: https://hackaday.io/project/173344-project-tracer.

[i.34] Palakurthi Shranav: "project-tracer". GitHub.com.

NOTE: Available at https://github.com/shraiwi/project-tracer.

[i.35] Palakurthi Shranav: "Tracer Demo" (video). June 22, 2020.

[i.36] Bettr: "TraceSigma".

NOTE: Available at: https://sites.google.com/view/tracestick.

[i.37] Bettr: "TraceSigma". GitHub.com.

NOTE: Available at: https://github.com/bettr-xyz.

[i.38] Engineers.SG: "TraceSigma" (see video from July 7, 2020).

[i.39] Conecta Industria: "Una empresa asturiana presenta un producto para el contact tracing en la Feria del Hogar de Gijón sin el uso de móvil ni geolocalización". August 7, 2020.

NOTE: Available at https://www.conectaindustria.es/tecnologia/002154/una-empresa-asturiana-presenta-un-producto-para-el-contact-tracing-en-la-feria-del-hogar-de-gijon-sin-el-uso-de-movil-ni-geolocalizacion.

[i.40] SRP: "La tecnología de ADN Mobile Solutions, cerca de ti en la lucha contra el COVID-19". Sociedad Regional de Promoción del Principado de Asturias. September 16, 2020.

NOTE: Available at https://www.srp.es/la-tecnologia-de-adn-mobile-solutions-cerca-de-ti-en-la-lucha-contra-el-covid-19/.

[i.41] Arenschield Laura. "Using your phone's microphone to track possible COVID-19 exposure". TechXplore.com. July 1, 2020.

NOTE: Available at https://techxplore.com/news/2020-07-microphone-track-covid-exposure.html.

[i.42] Luo Yuxiang, Cheng Zhang, Yunqi Zhang, Chaoshun Zuo, Dong Xuan, Zhiqiang Lin, Adam C. Champion and Ness Shroff: "ACOUSTIC-TURF: Acoustic-based Privacy-Preserving COVID-19 Contact Tracing". Cornell University. arXiv.org. June 23, 2020.

NOTE: Available at https://arxiv.org/abs/2006.13362.

[i.43] Yunqi Zhang; Luo, Yuxiang; Cheng Zhang; Chaoshun Zuo; Dong Xuan; Zhiqiang Lin; Adam C. Champion and Ness Shroff. "Technical Report. ACOUSTIC-TURF: Acoustic-based Privacy-Preserving COVID-19 Contact Tracing". June 23, 2020.

NOTE: Available at https://arxiv.org/pdf/2006.13362.pdf.

[i.44] Novak Ed, Zhuofan Tang and Qun Li: "Ultrasound proximity networking on smart mobile devices for IoT applications". IEEE Internet of Things Journal 6, 1 (2018), 399-409.

[i.45] Santagati, G. E. and T. Melodia: "A Software-Defined Ultrasonic Networking Framework for Wearable Devices". IEEE/ACM Transactions on Networking 25, 2, (2017) 960-973.

[i.46] Nandakumar, Rajalakshmi; Krishna Kant Chintalapudi; Venkat Padmanabhan and Ramarathnam Venkatesan: "Dhwani: secure peer-to-peer acoustic NFC". ACM SIGCOMM Computer Communication Review 43, 4 (2013), 63-74.

[i.47] Zhang Huanle, Wan Du, Pengfei Zhou, Mo Li and Prasant Mohapatra: "An acoustic-based encounter profiling system". IEEE Transactions on Mobile Computing 17, 8 (2017), 1750-1763.

[i.48] Loh Po-Shen (n.d.): "NOVID".

NOTE: Available at https://www.novid.org/.

[i.49] Foy Kylie: "Signs of Covid-19 may be hidden in speech signals". MIT News. July 8, 2020.

NOTE: Available at https://news.mit.edu/2020/signs-covid-19-may-be-hidden-speech-signals-0708?fbclid=IwAR2PAqm347cY_mQwYteCrDuAQENc5odij93RAIygMNmVhxIYu2VpUerPCcE.

[i.50] Quatieri, Thomas F; Tanya Talkar and Jeffrey S. Palmer: "A Framework for Biomarkers of COVID-19 Based on Coordination of Speech-Production Subsystems". IEEE Open Journal of Engineering in Medicine and Biology, Volume 1. May 29, 2020.

NOTE 1: Available at https://doi.org/10.1109/OJEMB.2020.2998051.

NOTE 2: Available at https://ieeexplore.ieee.org/document/9103574.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Bluetooth® low energy: low power wireless Personal Area Network (PAN) communication technology that can be used over a short distance to enable smart devices to communicate

contact tracing: essential measure to fight an ongoing pandemic with the purpose of identifying and managing the contacts of probable or confirmed cases to rapidly identify secondary cases that may arise after transmission from the primary known cases in order to intervene and interrupt further onward transmission

NOTE: Contact tracing is the term used to describe the overall public health strategy and actions involved in tracing and following up contacts. Mobile apps cannot be said to do 'contact tracing', but rather 'proximity tracking' and 'exposure notification'; i.e. tracking and alerting users who have been in close proximity with each other, which can support contact tracing.

Curve25519: state-of-the-art cryptographic function designed for use with the Diffie–Hellman key exchange protocol and suitable for a wide variety of applications

NOTE: It is one of the fastest elliptic curve cryptography (ECC) curves and is not covered by any known patents. The reference implementation is public domain software.

Diffie-Hellman key exchange protocol: method for safely distributing keys that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel

digital fragility: quality of an entity (organization, system, etc.) that determines its susceptibility to suffer an incident, of "digital" nature, that disturbs its activity (besides causing other consequences for people, assets or the environment); and of which possible materialization there is not always consciousness

exposure notification: feature of a mobile app that supports digital contact tracing by notifying to its user an exposure, above/below thresholds specific to each contact tracing system, to a person later diagnosed as probable or confirmed case

proximity tracking: feature of a mobile app that supports digital contact tracing by measuring Bluetooth® signal strength to determine whether two mobile devices were close enough together for their users to transmit the virus respectively, to get infected by the virus

SecNumCloud (formerly Secure Cloud): initiative by the French National Cybersecurity Agency (ANSSI), aiming to improve protection for public authorities and Operators of Vital Importance (OVIs)

NOTE: Launched in 2013, the idea under this quality seal was to create a label that demonstrated the high level of security met by those cloud solution providers serving strategic business and government agencies.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API	Application Programming Interface
APK	Android application PacKage

NOTE: Android® is a trademark of Google LLC.

CPU	Central Processing Unit
DP-3T	Decentralised Privacy-Preserving Proximity Tracing
E4P	Europe for Privacy-Preserving Pandemic Protection
EBID	Ephemeral Bluetooth® IDentifier
EMR	Electronic Medical Record
ENS	Exposure Notification System
ENX	Exposure Notification eXpress
EU	European Union
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GR	Group Report
GS	Group Specification
HMS	Huawei® Mobile Services
ID	IDentifier
IDPT	Interoperable Digital Proximity Tracing
IDPT-FP	Interoperable Digital Proximity Tracing - Full Protocol
I-EBID	Interoperable EBID
ISG	Industry Specification Group
NFC	Near Field Communications
NTP	Network Time Protocol
NUS	Near Ultra Sound
PACT	1. Private Automated Contact Tracing (East Coast PACT) 2. Privacy-sensitive protocols And mechanisms for mobile Contact Tracing (West Coast PACT)
PIA	Privacy Impact Analysis
PII	Personally Identifiable Information
QR	Quick Response [code]
RFID	Radio Frequency IDentification
RSSI	Received Signal Strength Indicator
SDK	Software Development Kit

TAN	Transaction/Telephone Authentication Number
UI	User Interface
UUID	Unique User IDentifier
UWB	Ultra Wide Band
UX	User eXperience

4 Current landscape of pandemic contact tracing

4.1 Overview: a universe of apps

For decades, public health services have promoted contact tracing in communicable disease control. This has made it a pillar of fight against pandemics. Traditionally, manual contact tracing has attempted to find all contacts of a confirmed case to test or monitor them for infection with the ultimate goal to save lives by stopping the spread of a disease through the location and isolation of new possible cases. Indeed, exhaustive manual pandemic contact tracing followed by isolation of infected individuals and immunization of their surrounding communities may prove to be more effective than universal immunization; but it is not always exempt of issues that may impact its effectiveness in addressing infectious diseases. Limitation in number of human monitors (tracers), the need for training, the difficulty to identify some contacts (e.g. people met in public transportation), etc. could undermine any tracing initiative. Here is where digital solutions arise as a support service making manual pandemic contact tracing more efficient.

A recent study (see [i.5]) by the Inter-American Development Bank Group's innovation laboratory (IDB Lab) has produced a census of several hundreds of COVID-19-related apps. Although not all of them are contact tracing apps, it constitutes **a true universe of apps**.

4.2 Manual pandemic contact tracing

Contact tracing to identify persons who potentially have been infected by known victims, and to isolate/treat those with secondary infections, is a proven way to contain an epidemic when full lock-down is not in place and inoculations are not available. The value in reducing the total number of infections in a given time depends strongly on the latency for symptoms and the mobility of the disease or people. Some sources (see [i.6]) have showed analytically that if latency is high (e.g. like 14 days in the average case for COVID-19) then effective contact tracing can be extremely helpful in containing outbreaks.

However, contact tracing also has resource costs. Conventional means of contact tracing requires interviewing the infected patient(s) regarding their lifestyle and sustained contacts (e.g. less than 2 metre distance for 15 minutes) using a long list of questions (see [i.7]) to trigger memories and elicit names/addresses. Many of the questions involve some invasion of privacy, justified by the medical risks. Persons to carry out the questionnaires are typically themselves put at higher risk of infection during the interview, and even more so during subsequent secondary and tertiary interviews where apparently healthy people may be contacted at their homes/workplace. The interviewers also need significant training to be effective (see [i.8]).

The reliance of conventional tracing on human memory, particularly of people who are sick or extremely worried, also reduces the completeness of the results. In a direct test within a Singapore hospital (see [i.9]), a comparison was made over two days between counting contacts of staff (162 persons) with patients (17 persons) based on patient medical records (EMRs) and a detailed interview of staff the next-day, compared to RFID-tracing of staff. The RFID method detected 54 contacts missed otherwise, the EMRs showed 99 contacts missed by RFID (but there is some doubt of accuracy of the records), and all together 257 contacts were found. Self-reporting by staff identified only 36 of those contacts. The lesson to learn is that, in a busy environment (here a hospital) the memory of contact with others may be very spotty, even under ideal conditions.

In a real-world example (see [i.10]) in Seoul in early May 2020, an outbreak of Covid-19 was detected in association with a nightclub district. By late May, using cell phone location data, credit card records, and lists of nightclub visitors, officials identified and carried out screening of more than 35 000 visitors. They detected 246 new infections: 96 primary cases, 32 secondary, and others that were 3, 4 and even 5 steps along the transmission chain from actual night club visitors. This example used some very broad-based location data (cell area) but can mainly be considered "conventional". The resource cost was obviously very high; however the mobility of the night-club visitors was also very high: the infected persons returned home to ten different areas across South Korea. Finding and isolating them rapidly was very important to avoid the need to impose lockdown on large parts of the country.

The above examples help to make clear that an automated, privacy-preserving method of detecting potential contagion and warning people to apply for screening could drastically reduce the investigative resource costs compared to conventional contact tracing and greatly increase the speed and completeness of case discovery. Speedy screening of persons likely to be infected is crucial to preventing the "chain reaction" of an outbreak (see [i.6]).

4.3 Digital pandemic contact tracing: initiatives per country

4.3.0 General

The following clauses provide a characterization (description) of a series of current digital contact tracing initiatives (apps), both alive and under development, given by country (in alphabetical order).

The aim to include a representative sample of the European landscape, as well as a few additional and relevant initiatives from abroad, has been among the very reasons for the final election of projects.

4.3.1 Austria (project "Stopp Corona")

Table 1: Austria's "Stopp Corona" project characterization

App's name	Stopp Corona.
Country	AT (Austria).
Official website (and source of this characterization) available at	https://www.stopp-corona.at/ (in German) https://www.roteskreuz.at/site/meet-the-stopp-corona-app/
Description	Stopp Corona utilizes the ENS framework. Therefore, the app mainly implements the user interface, the risk-score calculation, and the communication with the backend. The backend is based on the reference implementation provided by Google®. The backend regarding the exchange of the keys is hosted using Microsoft Azure. There is no external validation regarding the reported state (see below). To lower the risk of misuse, the reporting user has to provide a mobile phone number. He will receive a TAN, which he has to provide as a means for verification of the telephone number. The telephone number will be stored, to identify the reporting user in case of misuse. The telephone numbers are stored using an Austrian provider. One speciality is, that the app introduces three types of keys: • *red keys*: These are the usually submitted keys in the ENS approach, indicating that the reporting user was diagnosed COVID-19 by a physician. Users informed about a red exposure are asked to self-quarantine for 14 days. • *yellow keys*: In this case, the reporting user might be infected, but he only did a self-assessment by answering a questionnaire. This questionnaire is part of the app. The yellow state was introduced to shorten the time of informing other users. The reporting user is asked to do a COVID-19 test as soon as possible. Users informed about a yellow exposure are asked to self-quarantine for 7 days. • *green keys*: This is to indicate, that the reporting user wants to revoke some previously sent yellow or red keys. In order to authenticate key-state updates a random value (UUID) is sent together with the initial key upload. Updates are only accepted if the same random value is provided.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely. A user can freely decide to participate in the system. The [possibly] infected person can choose to disclose an [possibly] infection on a volunteering base.
Data processing legal basis	GDPR, Datenschutzgesetz (DSG), Epidemiegesetz, Privacy Shield (because of the usage of Microsoft Azure).
Data usage limitation	According to the app's privacy policy, data usage is limited to certain purposes.

Data destruction	Locally store data is deleted if the app is deinstalled. The phone number provided to receive the TAN will be deleted after 30 days. All data will be deleted after the end of the pandemic.
Data minimization	The user does not provide the Austrian Red Cross (ÖRK) with any data such as name, date of birth, etc. Only when submitting a report, a mobile phone number is provided in order to receive a TAN via SMS, which is used to release the report. The telephone number provided by the user is to be regarded as directly personal data, as the user can be contacted directly. It is planned to collect data for statistical purposes (number of key uploads, number of received EBIDs).
Data anonymization/pseudonymization	Exchanged keys are pseudonymous as they do not have any personal identifiers. When an infection is reported the phone number is recorded, to prevent misuse. Besides that, only a pseudonymous unique user ID (UUID) is known to the backend server.
Data subject rights	The user can revoke his agreement to the data collection at any time. Besides this, the user has the usual rights according to the GDPR.
Transparency	The source code for Android® and iOS apps as well as the backend are available. Some limited technical documentation regarding both, app and back-end's design and implementation, are available. The proximity tracing solution itself is a black box hidden in the operating system (services). A user gets informed about data collection and processing during the installation of the app.
Technical documentation available at	https://github.com/austrianredcross/stopp-corona-documentation (certain documentation seems to be outdated, since Austria followed at the beginning another approach, because the ENS framework was not available at the time).
Source code available at	https://github.com/austrianredcross

4.3.2 Estonia (project "Hoia")

Table 2: Estonia's "Hoia" project characterization

App's name	Hoia.
Country	EE (Estonia).
Official website (and source of this characterization) available at	https://hoia.me/en/
Description	Hoia lets you quickly find out about possible close contact with a COVID-19 infected person, allowing you to take steps to protect your own health and the health of others. Phones that use the app register the Bluetooth® signals from other nearby phones. If the signal is sufficiently close and long enough, an anonymous code referring to a close contact will be stored in their phone. If a person now confirms their infection with the Hoia app, the anonymous codes on their device will be uploaded to a central server where all users can download them. It is not possible to identify a person based on an anonymous code. The user's phone compares whether the infected person's anonymous code matches a code previously stored on their phone. If so, the user is considered to be a close contact and they will be notified with instructions. It will not be revealed to the user who the infected person was with whom they were in contact with, or any other information that would allow the indirect identification of the infected person. Only subjects with a confirmed test result can mark themselves as infected. Users use e-IDAS compliant mobile phone authentication technology to confirm their person and bind the test result to the keys in the protocol.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS + DP-3T Software Development Kits (SDK).
Voluntary nature	Entirely (this is stressed in all communication). A user is free to (not) download the application and set it up (giving consents to relevant phone operating system APIs). A user is free to (not) mark themselves as infected (having multiple chances to cancel the process).

	For more information, please, refer to item 4 in the privacy policy. URL: https://hoia.me/privacy/
Data processing legal basis	The Hoia app does not process personally identifiable information (PII). The backend processes infection confirmations and handles PII. The following bases are used: • Consent. • EU General Data Protection Regulation (GDPR). • Estonian Personal Data Protection Act. Available at: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide. • Estonian Health Services Organisation Act that regulates the person's ability to give consent to data transfer in collaboration with the Health Information System regulation. • Available at: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518052020003/consolide
Data usage limitation	The app has two main functions: notifying risk of exposure (exposure notifications) and letting the user marking herself as infected. For more information, please, refer to items 9 and 11 in the privacy policy. URL: https://hoia.me/privacy/
Data destruction	Data is destroyed 14 days after creation; the user can also delete data in the phone (whenever she prefers). For more information, please, refer to items 10 and 13 in the privacy policy. URL: https://hoia.me/privacy/
Data minimization	The application and backend follow privacy-by-design principles. The app does only one thing and nothing else (e.g. no epidemiological data upload is currently implemented at all). For more information, please, refer to items 6, 9 and 11 in the privacy policy. URL: https://hoia.me/privacy/
Data anonymization/pseudonymization	The app follows the decentralized design from DP-3T and ENS, relying heavily on cryptographic techniques to ensure anonymity for as much data to as many stakeholders as feasible.
Data subject rights	The user has the right to stop using the app, to revoke the app's access to the Exposure Notification APIs and other phone features, etc. For more information, please, refer to items 13 and 14 in the privacy policy. URL: https://hoia.me/privacy/
Transparency	Source code and documentation are open source. The DP-3T SDK components of the app and backend are open source. The Apple® /Google® operating system components are not open source (while technical documentation is available and open source clones exists). For more information, please, refer to the privacy policy. URL: https://hoia.me/privacy/
Technical documentation available at	https://koodivaramu.eesti.ee/tehik/hoia/documentation (documentation -currently in Estonian- also includes a security analysis). Specific DP-3T and ENS documentation may apply as well to parts of the system.
Source code available at	https://koodivaramu.eesti.ee/tehik/hoia

4.3.3 Finland (project "Koronavilkku")

Table 3: Finland's "Koronavilkku" project characterization

App's name	Koronavilkku.
Country	FI (Finland).
Official website (and source of this characterization) available at	https://koronavilkku.fi/en/

Description	Koronavilkku is a contact tracing app produced by the Finnish Institute for Health and Welfare (THL) to help you find out whether you may have been exposed to coronavirus. If you have a coronavirus test and are diagnosed as infected, you can use the app to share this anonymously with those you have been in close contact with. Your privacy is strongly protected.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely. Use of Koronavilkku is not mandatory and any user can stop using the app at any time by deleting it from her phone. For more information, please, refer to the Koronavilkku official website. URL: https://koronavilkku.fi/en/#yksityisyys If an app user is diagnosed by a healthcare professional as having COVID-19 infection, the user receives a single-use unlock code that the user can tap into the app at their own discretion. This allows other users of the app to be notified of potential exposure to coronavirus. The information does not allow users to identify persons infected with or exposed to the virus. If the app sends the user an alert of potential exposure, the user can, at her own discretion, report potential exposure to a healthcare professional by phone. The app can also redirect the user to a separate health check service web page. The app does not send information about exposure or any other identifiable information to healthcare professionals or other authorities. For more information, please, refer to the privacy policy. URL: https://koronavilkku.fi/en/privacy/
Data processing legal basis	THL's duties are laid down in the Act on the National Institute for Health and Welfare (668/2008). The use and maintenance of the app are laid down in sections 43a to 43h of the Communicable Diseases Act (1227/2016). The lawful basis for processing PII under the EU's GDPR is: • Performance of a task carried out in the public interest (Article 6(1)(e) of the GDPR and section 4(2) of the Finnish Data Protection Act (1050/2018) In addition, the processing of sensitive personal data is based on the special provision under Article 9(2) of the GDPR and section 6 of the Finnish Data Protection Act: • Processing is necessary for reasons of public interest in the area of public health (Article 9(2)(i) of the GDPR). For more information, please, refer to the privacy policy. URL: https://koronavilkku.fi/en/privacy/
Data usage limitation	The Finnish Communicable Diseases Act limits the usage of gathered data to contact tracing purposes. For more information, please, refer to the original Finnish text (no official English translation is available so far). URL: https://www.finlex.fi/fi/laki/ajantasa/2016/20161227#L4aP43c
Data destruction	A user can, at any time, remove the app from her phone whereupon all pseudonymous codes stored in the phone will automatically be removed. Any pseudonymous codes in the back-end system will be automatically removed, too, within 21 days. For more information, please, refer to the privacy policy. URL: https://koronavilkku.fi/en/privacy/ Legislation allowing information retention is currently in force until 31 March 2021. For more information, please, refer to the Koronavilkku's FAQ. URL: https://koronavilkku.fi/en/faq/

Data minimization	The mobile app stores the following data in the user's own mobile device: • The user's own pseudonymous codes. • The pseudonymous codes of others the user comes into close contact with and the associated data relating to the length, time and Bluetooth® signal strength of such contacts. • The pseudonymous codes of the user reporting their infection. • The information on potential exposure, received by the user. • An unlock code (not stored but processed). The back-end system saves the following data: • The pseudonymous codes of the users reporting their infection. The professional user interface component of the solution temporarily stores: • The telephone number of that user tested positive, for the purpose of sending a single-use unlock code to the user's mobile phone. For more information, please, refer to the privacy policy. URL: https://koronavilkku.fi/en/privacy/
Data anonymization/pseudonymization	Koronavilkku does not store any user's name, date of birth or contact information. It cannot identify her or the people she come into contact with. The app does not collect information about where you are. The app works using regularly changing and randomly generated codes. Users of the app cannot be directly identified from these codes. All communication between Koronavilkku and the server is encrypted. The information is stored anonymously on a server managed by the Social Insurance Institution (Kela) in Finland. For more information, please, refer to the Koronavilkku's FAQ. URL: https://koronavilkku.fi/en/faq/

Data subject rights	Right to withdraw consent: • The processing of personal data is based on the Communicable Diseases Act. A user can, at any time, remove the app from her phone whereupon all pseudonymous codes stored in the phone will automatically be removed. Any pseudonymous codes in the back-end system are also automatically removed within 21 days. THL is not able to identify the user from pseudonymous code data. Right to access data concerning a user: • A user has the right to know whether THL is processing personal data concerning her. A user also has the right to know what personal data concerning her is processed and how. A user also has the right to receive a copy of the personal data concerning her insofar as providing her with a copy does not adversely affect the rights and freedoms of others; or if THL does not have legal grounds for refusing to disclose the data. Where THL is unable to identify a user from the data, the right to access cannot apply because it is not possible. Right to rectification of data: • A user basically has a right to have inaccurate or incorrect data rectified. Where THL is unable to identify a user from the data, the right to rectification of data can not apply because it will not be possible. Right to erasure of your data: • A user can at any time remove the app, whereupon any pseudonymous code data in her phone and back-end system will be automatically deleted within 21 days at the latest. THL is not able to identify a user from pseudonymous code data. Right to restrict processing: • A user may have the right to restrict the processing of her personal data in cases laid down by law. The right to restrict processing may exists, for instance, if a user believes that the personal data concerning her is inaccurate, it is being processed unlawfully or the user has objected to the processing of her data. In this case, data may be processes only with the user's consent, where necessary for the establishment, exercise or defence of legal claims, or where it is in the general interest or essential to protect another person's rights. Where THL is unable to identify a user from the data, the right to restrict processing cannot apply because it will be not possible. Right to object to the processing of personal data: • A user may have the right to object to the processing of her personal data in cases laid down by law. The right to object may exist, for instance, if the processing is associated with automatic decision-making based on profiling or if the data is used for direct marketing purposes. Right to refer a matter to the supervisory authority: • A user has the right to request the Data Protection Ombudsman to assess the lawfulness of THL's activities. For more information, please, refer to the privacy policy. See https://koronavilkku.fi/en/privacy/
Transparency	Koronavilkku's source code and documentation are open source (see below). Koronavilkku's privacy policy is available at: https://koronavilkku.fi/en/privacy/ A security assessment has also been done that is available at: https://thl.fi/documents/533963/5860112/Johdon_tiivistelm%C3%A4-Koronavilkku-arviointi_25.08.2020.pdf/221c17db-05dd-4222-c001-2124ec9cbbd8?t=1598597462979
Technical documentation available at	https://github.com/THLfi/koronavilkku-android https://github.com/THLfi/koronavilkku-ios https://github.com/THLfi/koronavilkku-backend
Source code available at	https://github.com/THLfi/koronavilkku-android https://github.com/THLfi/koronavilkku-ios https://github.com/THLfi/koronavilkku-backend

4.3.4 France (project "StopCovid")

Table 4: France's "StopCovid" project characterization

App's name	StopCovid.
Country	FR (France).
Official website (and source of this characterization) available at	https://stopcovid.gouv.fr/ https://www.economie.gouv.fr/stopcovid
Description	StopCovid is the official French digital contact tracing application based on proximity detection that uses the ROBERT protocol. It was developed by a consortium led by Inria involving, among others, ANSSI (the French cybersecurity agency), INSERM (the French public research institution focused on human health and medical research) and Santé Publique France (the French public health agency). Positive COVID-19 tests come with a QR code that the user can scan with the application to notify its status. The backend is running on a SecNumCloud-certified solution (as defined by ANSSI), ensuring the highest level of security and that the data is stored in Europe and that no other jurisdiction can access it.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ROBERT.
Voluntary nature	Entirely. A user freely decides to participate in the system. A COVID-19 diagnosed person freely chooses to disclose its status. StopCovid can be deleted at any time.
Data processing legal basis	GDPR and relevant French legislation. CNIL (the French national data protection authority) was consulted.
Data usage limitation	Limited to the purpose of the application: contact tracing.
Data destruction	Yes.
Data minimization	Yes.
Data anonymization/pseudonymization	Cf. ROBERT protocol. Users are pseudonymized.
Data subject rights	According to GDPR.
Transparency	StopCovid's source code and documentation are open code (see below).
Technical documentation available at	https://gitlab.inria.fr/stopcovid19/accueil
Source code available at	https://gitlab.inria.fr/stopcovid19/accueil
NOTE: At the time of closing the edition of the present document, the French authorities have just released "TousAntiCovid" a new contact tracing app substituting "StopCovid". The new app was released on October 22, 2020.	

4.3.5 Germany (project "Corona-Warn-App")

Table 5: Germany's "Corona-Warn-App" project characterization

App's name	Corona-Warn-App
Country	DE (Germany)
Official website (and source of this characterization) available at	https://www.coronawarn.app/en/
Description	Corona-Warn-App's overall approach is based on the ENS API. Therefore, the app just implements the user interface, the risk-score calculation, and the communication with the back-end system (including the authorization of the key upload). The app as well as the back-end components are made open source. The back-end is operated by Deutsche Telekom using their Open Telekom Cloud (https://open-telekom-cloud.com/). Therefore, all the backend servers are currently located in Germany. Data owner is the Robert Koch Institute (https://www.rki.de/). Besides proximity tracing the app additionally allows to receive information regarding the result of a COVID-19 test.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely.

Data processing legal basis	GDPR, German Data Protection laws and possibly other laws like Infektionsschutzgesetz. No specific law for proximity tracing.
Data usage limitation	According to the app's privacy policy, data usage is limited to certain purposes.
Data destruction	Data locally stored by the app can be deleted any time on user's request. Data shared with the backend will be deleted by the backend system at latest 21 days after submission. Since certain data is made publicly available by the backend, its destruction is out of the control of the system.
Data minimization	To reduce the amount of collected and processed data certain measures are applied, still it is unclear if the reaming amount of collected and processed data can be considered minimal.
Data anonymization/pseudonymization	The emitted ephemeral Bluetooth® IDs are pseudonymized. Communication with the backend is not anonymized.
Data subject rights	A user has the right to withdraw its consent to the data collection/processing at any time. This will affect any future activity. User rights as specified in the GDPR are usually not effective, since no PII is collected.
Transparency	The results of a privacy impact analysis (PIA) done by the German Data Protection regulator is available. URL: https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf. Corona-Warn-App's users get informed about data collection and processing during the installation of the app. The proximity tracing solution itself is a black box hidden in the operating system (services). Corona-Warn-App's source code and documentation regarding both, app and back-end's design and implementation, are available (see below).
Technical documentation available at	https://github.com/corona-warn-app/cwa-documentation https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md (solution architecture.)
Source code available at	https://github.com/corona-warn-app

4.3.6 India (project "Aarogya Setu")

Table 6: India's "Aarogya Setu" project characterization

App's name	Aarogya Setu.
Country	IN (India).
Official website (and source of this characterization) available at	https://www.mygov.in/aarogya-setu-app/
Description	Aarogya Setu is an app to primarily spread awareness regarding health services with an imminent focus on COVID-19. It uses a phone's GPS and Bluetooth® to detect the proximity to neighbourhoods which have detected infected patients as well as do contact tracing. The app also provides information on how many users are infected in a given geography and based on movement attempts to predict the risk profile of an end-user. It provides options to contribute to the governments relief program as well as informs users on how effective government methods to control COVID-19 have been.
Type	Exposure notification by tracking user's movement in infected areas as well as Bluetooth® based contact tracing.
Technology	GPS / Bluetooth® Low Energy.
Method	Proprietary (the contact tracing mechanism is not shared in public domain).
Voluntary nature	Entirely.

Data processing legal basis	No specific law for proximity tracing.
Data usage limitation	The policy mentions data is deleted after a period of time and data is not shared with any other government department.
Data destruction	The policy mentions data is deleted after a period of time and data is not shared with any other government department.
Data minimization	
Data anonymization/pseudonymization	The emitted ephemeral Bluetooth® IDs are **NOT** pseudonymized. Communication with the back-end links to a mobile number and hence may not be anonymized.
Data subject rights	Not clear.
Transparency	The proximity tracing solution itself is a black box hidden in the operating system (services). The back-end mechanism, server details and data access mechanisms are not transparent. Reference source code for the Android® implementation has been shared (see below).
Technical documentation available at	https://github.com/nic-delhi/AarogyaSetu_Android
Source code available at	https://github.com/nic-delhi/AarogyaSetu_Android

4.3.7 Ireland (project "COVID Tracker")

Table 7: Ireland's "COVID Tracker" project characterization

App's name	COVID Tracker.
Country	IE (Ireland).
Official website (and source of this characterization) available at	https://covidtracker.gov.ie
Description	COVID Tracker is a free app for mobile phones aiming to help to protect each other and slow the spread of COVID-19 in Ireland. The app has three main functions: • contact tracing; • symptom tracking; and • news & information. The first time anyone uses the app they are prompted to allow the app to collect and share the anonymous data transmitted by nearby mobile phones that also have the app installed. Then they are asked how they would like the health authorities to contact them. If their phone sees that they have been in close contact, i.e. too close (within 2 metres of each other) for too long (more than 15 minutes), with someone who has tested positive, a healthcare worker can call them if they have chosen to share their contact phone number. The app takes advantage of different capabilities of mobile operating systems: • Apple® & Google® have developed a method, ENS, that allows specific government-only COVID-19 apps to make use of Bluetooth® technology on phones that would otherwise not be available. • Thanks to Bluetooth® and through continuous scanning, each mobile device logs the nearby phone at least every 5 minutes. This activity happens the whole day, in the background, on users' phones.
Type	Exposure notification in support to contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely.
Data processing legal basis	The legal basis for the processing of the data is consent - namely Article 6(1)(a) of the GDPR for the processing of personal data and Article 9(2)(a) of the GDPR for the processing of special categories of personal data, in this case health related data.
Data usage limitation	The app has the purpose of supporting the Irish national public health response and members of the public during the COVID-19 crisis.
Data destruction	Personal data is held for: • Exposure Notification identifiers: 14 days. • Diagnosis keys uploaded to the back-end: 14 days.

	• Diagnosis keys on the mobile device: as long as they are necessary to perform a match check. • COVID Check-In information: – on the device: 28 days; and – uploaded to the back-end: 1 day. • App metrics: a minimum of 7 years.
Data minimization	The app uses about 1MB of data per week (equivalent to 6 minutes of Internet browsing).
Data anonymization/pseudonymization	COVID Tracker uses the Exposure Notification System (ENS) developed by Apple® and Google® as it has been pointed out above. This allows phones to share anonymous IDs using Bluetooth®. These IDs contain information about how close someone was to other app user(-s) and how long she was close to them. The anonymous IDs are codes made up of letters and numbers. An app user never sees them. They cannot be used to identify users or their phones. Using an anonymous ID means any information is collected anonymously. No one will ever know your personal details unless you choose to share them. This includes Apple® , Google® and the Irish Health Service Executive.
Data subject rights	Any user has the following rights as a data subject under the GDPR in respect of her personal data that are processed by the app: • Request information on and access to her personal data. • Request correction of the personal data that the health authorities hold about her. • Request erasure of her personal data. • Object to processing of her personal data. • Object to automated decision-making including profiling. • Request the restriction of processing of her personal data. • Request transfer of her personal information in an electronic and structured form to her or to another party. Any user also has the right to make a complaint before the Irish Data Protection Commission.
Transparency	The results of a Privacy Impact Analysis (PIA) done by the Irish Data Protection regulator is available. URL: https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%2026.06.2020.pdf Additionally, and as part of the COVID Tracker initiative's commitment to transparency, the following information is available: • Data Protection Information Notice. URL: https://covidtracker.gov.ie/privacy-and-data/data-protection/ • Privacy designs. URL: https://github.com/HSEIreland/covidtracker-documentation/tree/master/documentation/privacy COVID Tracker's source code and documentation are open code (see below).
Technical documentation available at	https://github.com/HSEIreland/
Source code available at	https://github.com/HSEIreland/covid-tracker-app

4.3.8 Italy (project "Immuni")

Table 8: Italy's "Inmuni" project characterization

App's name	Inmuni.
Country	IT (Italy).
Official website (and source of this characterization) available at	https://www.immuni.italia.it/ (available in Italian, English, French, German & Spanish).
Description	Inmuni sends a notification to people who were in close contact with a user who tested positive for the COVID-19 virus, alerting them of the risk of infection. Thanks to Bluetooth® Low Energy technology, this takes place without the app gathering any data on the identity or the location of its users. The app has been designed and developed while taking great care to safeguard user privacy. Any data, collected and managed by the Ministry of Health and by public bodies, is stored on servers located in Italy. All the data and app connections with the server are protected. Where individuals are tested positive to COVID-19 they can upload the temporary exposure keys to the server authenticating with a one-time code given to the user by a health operator.
Type	Exposure notification in support to contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely. Inmuni's installation, its activation and the transmission of the keys to the server (if tested positive) are all voluntary actions.
Data processing legal basis	
Data usage limitation	Yes, the data can be further used only for health statistics and pseudonymised.
Data destruction	Yes, the latest on December 31, 2020 data will be destroyed or fully anonymized.
Data minimization	Yes, only the minimum set of information is used.
Data anonymization/pseudonymization	Yes, the data can be further used only for health statistics and pseudonymized.
Data subject rights	
Transparency	Source code and technical documentation are available (see below).
Technical documentation available at	https://github.com/immuni-app/immuni-documentation (English only)
Source code available at	https://github.com/immuni-app

4.3.9 Japan (project "COCOA")

Table 9: Japan's "COCOA" project characterization

App's name	COCOA.
Country	JP (Japan).
Official website (and source of this characterization) available at	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html (Japanese only).
Description	This app uses the short-range communication function (Bluetooth®) on smartphones upon user approval to receive notifications about the possibility of contact with a person who has tested positive for the novel coronavirus, while ensuring pseudonymity for the user's privacy. Users can receive support, such as testing from a public health centre, sooner, by knowing that they might have been in contact with someone who has tested positive. The more users, the more effective it will be in preventing the spread of infection. For more information, please, refer to the "Request to install the COVID-19 Contact-Confirming Application (COCOA)" and FAQ brochure (English edition). URL: https://www.mhlw.go.jp/content/10900000/000647649.pdf
Type	Contact Confirmation Application.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely.

Data processing legal basis	Japanese Privacy Law.
Data usage limitation	According to the app's privacy policy, data usage is limited to certain purposes.
Data destruction	Data locally stored by the app can be deleted any time on user's request. Data shared with the backend will be deleted by the backend system at latest 14 days after submission. Since certain data is made publicly available by the backend, its destruction is out of the control of the system.
Data minimization	To reduce the amount of collected and processed data certain measures are applied, still it is unclear if the reaming amount of collected and processed data can be considered minimal.
Data anonymization/pseudonymization	The emitted ephemeral Bluetooth® IDs are pseudonymised. Communication with the backend is not anonymized.
Data subject rights	A user has the right to withdraw its consent to the data collection/processing at any time. This will affect any future activity.
Transparency	No. Source codes for Apps and backend system are not available in public (see below).
Technical documentation available at	https://cio.go.jp/sites/default/files/uploads/documents/techteam_20200526_01.pdf (in Japanese)
Source code available at	No. Source code for the app and backend system are not publicly available.

4.3.10 Lithuania (project "Korona Stop LT")

Table 10: Lithuania's "Korona Stop LT" project characterization

App's name	Korona Stop LT.
Country	LT (Lithuania).
Official website (and source of this characterization) available at	https://koronastop.lrv.lt/
Description	Korona Stop LT is the official COVID-19 exposure notification app for Lithuania. The installation of the app is voluntary. The app has contact tracing and warning functionalities to identify the persons that have been in contact with a person infected by COVID-19 and to inform him/her (without revealing personal data) about appropriate next steps, such as self-quarantine, testing or providing advice on what to do in case of symptoms (the aim is not to follow the movements of individuals or to enforce prescriptions). It uses Bluetooth® Low Energy technology and Exposure Notification API to ensure privacy and security. The proximity data is generated and stored in encrypted and pseudonymized format. If person infected with COVID-19 chooses to inform close contacts, he/she has to get confirmation from National Public Health Center under the Ministry of Health (NPHC). The app does not record GPS data even if GPS is switched on and does not track users location. Users are able to uninstall the app at any time.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely. Installation and use of the app are completely voluntary.
Data processing legal basis	Personal data is processed by a person's consent in accordance with GDPR Article 6(1) (a) and Article 9(2) (a). A user has a right to withdraw his/her given consent at any time but this does not affect the lawfulness of the processing based on consent before its withdrawal.
Data usage limitation	The data is processed for the purposes of technical infrastructure protection and maintenance. The app does not collect data that allows to identify users or to find out about their health or location.

Data destruction	The list of random IDs of users who anonymously reported that they are infected will be deleted from the app immediately. Random IDs are automatically deleted from smartphone's exposure log after 14 days. It may also be possible, using the functionality provided by Apple® and Google®, to delete data manually in smartphone's system settings.
Data minimization	The app is designed to process as little personal data as possible.
Data anonymization/pseudonymization	Exposure logging functionality uses randomly generated identification numbers (random IDs) which smartphone's exchanges via Bluetooth® Low Energy. Random IDs as well as the other contact data (date and time of the contact, duration of the contact, signal strength of the contact and encrypted metadata) are recorded by smartphones in an exposure log and are stored there for 14 days. IP address is masked and not used within the app's back-end system.
Data subject rights	The user can revoke his agreement to the data collection at any time. Besides this, the user has the usual rights according to the GDPR.
Transparency	Users are informed about data privacy during the installation of the app. It is not clear whether the source code for Android® and iOS apps as well as the backend are available. Some limited technical documentation regarding both, app and back-end's design and implementation, are available.
Technical documentation available at	N/A
Source code available at	N/A

4.3.11 Poland (project "ProteGO Safe")

Table 11: Poland's "ProteGO Safe" project characterization

App's name	ProteGO Safe.
Country	PL (Poland).
Official website (and source of this characterization) available at	https://www.gov.pl/web/protegosafe
Description	ProteGO Safe is the official Polish application for tracking contact with the coronavirus, issued by the Ministry of Digitization in cooperation with the Chief Sanitary Inspectorate. The application is intended for use in Poland.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely. The user anonymously, without providing any data or enabling any identification, installs the app on the device with the Android® or iOS operating system.
Data processing legal basis	Personal data are processed on the basis of Article 6 section 1 lit. (e) of GDPR in connection with a task carried out in the public interest consisting in preventing, counteracting and combating COVID-19 resulting from Articles 1, 2, 3, 6 and 8a sections 1, 4 and 5 of the Act of 14 March 1985 on the State Sanitary Inspection (Journal of Laws of 2019, item 59). Personal data regarding medical data are also processed pursuant to Article 9 paragraph 2 lit. and GDPR in connection with the public task of preventing, counteracting and combating COVID-19 resulting from Articles 1, 2, 3, 6 and 8a sections 1, 4 and 5 of the Act of 14 March 1985 on the State Sanitary Inspection (Journal of Laws of 2019, item 59) - processing is necessary for reasons related to the public interest in the field of public health, such as protection against serious cross-border health threats under the law of the Member State.
Data usage limitation	The user opens the app and displays information about the way it works and the necessary consents / permissions (acceptance of the Terms and the Privacy Policy). The app is designed in a way that prevents Ministry of Digitization, Chief Sanitary Inspectorate or any other entity from changing the purpose of processing.

Data destruction	Contact details are deleted from the user's device after 14 days [parameter].
Data minimization	The app pays particular attention to ensure the highest privacy standards. Adopted solutions ensure the support for the health authorities in fighting the pandemic while using the minimal set of data, necessary to accomplish that goal.
Data anonymisation/pseudonymisation	Distributed system: 1) Data is stored on users' devices. All information (entries in the Health Journal), as well as the history of devices encountered are stored on users' devices and analysed there. 2) Data entered into STOP COVID - ProteGO Safe allows users to remain anonymous. It is not necessary to register or provide any identifying information. In addition to installing the application, the user only provides his nickname, which can be any, and its only purpose is user comfort. 3) Only people who are medically verified as patients with COVID-19 will be able to initiate the process of sending their Diagnosed Keys (prior to this, Contact Center has to reach the Patient to get a consent to enable appropriate export gateway for data upload - it is required - this consent is made voluntarily by a sick person, thus Contact Center has no means nor rights to do so on behalf of the patient by itself) so that they can send a warning to other users.
Data subject rights	According to GDPR. In particular: 1) pursuant to Article.15 GDPR, the right to access Personal Data; 2) pursuant to Article 16 GDPR, the right to rectify Personal Data; 3) pursuant to Article 17 GDPR, the right to delete Personal Data; 4) pursuant to Article 18 GDPR, the right to request the Administrator to limit the Processing of Personal Data, subject to the cases referred to in Article 18 section 2 GDPR; 5) pursuant to Article 21 GDPR, the right to object to the Processing of Personal Data. In order to exercise the rights, data subject have to use the appropriate STOP COVID - ProteGO Safe functionalities.
Transparency	ProteGO Safe's source code and documentation are open code (see below).
Technical documentation available at	https://github.com/ProteGO-Safe/specs/blob/master/README-ENG.md
Source code available at	https://github.com/ProteGO-Safe

4.3.12 Singapore (project "Trace Together")

Table 12: Singapore's "Trace Together" project characterization

App's name	Trace Together.
Country	SG (Singapore).
Official website (and source of this characterization) available at	https://tracetogether.gov.sg/
Description	Trace Together is the implementation of the Blue Trace protocol. The app was developed by the Government Technology Agency and released on 20 March 2020. The app is available for Android® and iOS. A reference source code has been released on github, however the app on playstore is not same as the one hosted on github.
Type	Exposure notification in support to contact tracing.
Technology	Bluetooth® Low Energy.
Method	Blue Trace.
Voluntary nature	The app has been made mandatory for some section of residents.
Data processing legal basis	Singaporean domestic privacy regulation.
Data usage limitation	Data will only be used for COVID-19 contact tracing.
Data destruction	Data is retained only for a limited time.
Data minimization	

Data anonymization/pseudonymization	The app requires users to register and hence may not be completely anonymous.
Data subject rights	
Transparency	Trace Together's source code and documentation are open code (see below).
Technical documentation available at	https://github.com/opentrace-community https://www.tracetogether.gov.sg/common/privacystatement
Source code available at	https://github.com/opentrace-community

4.3.13 Spain (project "Radar COVID")

Table 13: Spain's "Radar COVID" project characterization

App's name	Radar COVID.
Country	ES (Spain).
Official website (and source of this characterization) available at	https://radarcovid.gob.es/
Description	Spanish national contact tracing app.
Type	Exposure notification in support to contact tracing (decentralized).
Technology	Bluetooth® Low Energy.
Method	ENS.
Voluntary nature	Entirely. Both adoption and notification of confirmed case based on PCR+.
Data processing legal basis	Explicit consent of the terms of use and privacy policy.
Data usage limitation	The app does not process any personal data. The Rolling Proximity identifiers (RPI) and Temporary Exposure Keys (TEK) are limited to contact tracing purposes following the DP-3T principles.
Data destruction	Local data (TEK/RPI) can be deleted at user's request and is deleted after 14 days otherwise. Central data (infected TEKs) are deleted after 14 days.
Data minimization	Only data for contact tracing purposes (TEK/RPI) is collected.
Data anonymisation/pseudonymisation	Rolling Bluetooth® identifiers could be considered as pseudonymized data.
Data subject rights	No personal data is collected, so GDPR rights are not applicable. Users can erase local data and/or uninstall the app at any time.
Transparency	Radar COVID's source code and documentation are open code (see below).
Technical documentation available at	http://github.com/radarcovid
Source code available at	http://github.com/radarcovid

4.3.14 Switzerland (project "SwissCovid")

Table 14: Switzerland's "SwissCovid" project characterization

App's name	SwissCovid.
Country	CH (Switzerland).
Official website (and source of this characterization) available at	https://foph-coronavirus.ch/swisscovid-app/ https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html

Description	SwissCovid represents Switzerland's effort in digital contact tracing. The app mainly implements the user interface and the communication with the backend. The backend is based on the reference implementation provided by DP3-T and run by the Federal Office of Public Health (FOPH), although per law, a 3rd party provider can be used. Google® & Apple® ENS is a de-facto standard based on DP-3T core concepts, at least for the device side. DP-3T is not an official body but a collection of top academic researchers, mainly from ETH/EPFL, who have a lot of trust from the Swiss government as part of how they are organized/funded. 20 % of Swiss population is using the app as of September 2020.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	ENS + DP-3T.
Voluntary nature	Entirely. A user can freely decide to participate in the system. The [possibly] infected person can choose to disclose a [possibly] infection on a volunteering base as defined in the legal basis below.
Data processing legal basis	According to "Ordinance of 24 June 2020 on the Proximity Tracing System for the Sars-CoV-2 coronavirus". For more information, please, refer to the portal of the Swiss government. URL: https://www.admin.ch/opc/de/classified-compilation/20201730/index.html
Data usage limitation	Anonymized data is provided to the Federal Office of Statistics.
Data destruction	14 days on app and backend. 24h. in the infection code management system.
Data minimization	The user does not provide the FOPH with any data such as name, date of birth, etc. Only when submitting a report, the IP address can be possibly stored and used to identify the person. Logs of such traffic are to be deleted after 7 days.
Data anonymization/pseudonymization	Exchanged IDs are derived from a private key which does not have any personal identifiers and changes at least every day.
Data subject rights	
Transparency	DP-3T is open source but ENS is not, so key generation and safekeeping cannot be verified by an independent body.
Technical documentation available at	https://github.com/DP-3T/documents (certain documentation seems to be outdated, since DP-3T was developed before ENS).
Source code available at	https://github.com/DP-3T/dp3t-app-android-ch

4.3.15 United States (project "CoEpi")

Table 15: United States' "CoEpi" project characterization

App's name	CoEpi
Country	US (United States)
Official website (and source of this characterization) available at	https://www.coepi.org
Description	CoEpi is a privacy-first system for anonymous Bluetooth® proximity-based exposure alerting based on voluntary symptom sharing.
Type	Exposure notification in support of contact tracing.
Technology	Bluetooth® Low Energy.
Method	TCN.
Voluntary nature	Entirely. CoEpi takes a privacy-first approach: users are anonymous and opt-in to ANY sharing of data beyond their local device.

Data processing legal basis	
Data usage limitation	
Data destruction	
Data minimization	
Data anonymization/pseudonymization	
Data subject rights	
Transparency	CoEpi is an open source project that is actively collaborating with others on a shared backend and Bluetooth® protocol so these apps can 'see' each other as devices, expanding the impact of CoEpi. CoEpi is doing this open source so individuals can investigate code to decide if it is trustworthy.
Technical documentation available at	https://github.com/Co-Epi
Source code available at	https://github.com/Co-Epi/app-android https://github.com/Co-Epi/app-ios

4.3.16 Summary

Table 16 shows a summary of some of the most relevant characteristics of the apps included in the current analysis.

Table 16: Summary of apps, per country

Country	Name	Promoter/health authority	Official site	Language	Approach	Os supported	Method	Transparency	PIA	Voluntary
AT	Stopp Corona	Federal Ministry of Health	https://www.stopp-corona.at/	DE	Decentralized	Android® / iOS	ENS	Doc & Code		Entirely
EE	Hoia	Estonian Health Board	https://www.hoia.me/en/	EN, EE	Decentralized	Android® / iOS	ENS	Doc & Code		Entirely
FI	Koronavilkku	Finnish Institute for Health and Welfare	https://koronavilkku.fi/en/	EN, FI, SV	Decentralized	Android® / iOS	ENS	Doc & Code		Entirely
FR	StopCovid	Ministry for Solidarity and Health	https://stopcovid.gouv.fr/	FR	Centralized	Android® / iOS	ROBERT	Doc & Code		Entirely
DE	Corona-Warn-App	The Robert Koch Institute	https://www.coronawarn.app/en/	EN, DE	Decentralized	Android® / iOS	ENS	Doc & Code	Yes	Entirely
IN	Aarogya Setu	Ministry of Health and Family Welfare	https://aarogyasetu.gov.in/	EN	Decentralized	Android® / iOS / KaiOS	PROPRIETARY	Partial		Entirely
IE	COVID Tracker	Health Service Executive	https://covidtracker.gov.ie/	EN	Decentralized	Android® / iOS	ENS	Doc & Code	Yes	Entirely
IT	Inmuni	Ministry of Health	https://www.immuni.italia.it/	EN, IT, DE, ES, FR	Decentralized	Android® / iOS	PRONTO-C	Doc & Code		Entirely
JP	COCOA	Ministry of Health, Labour and Welfare	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html	EN, JP	Decentralized	Android® / iOS	ENS	Doc		Entirely
LT	Korona Stop LT	Gov't of the Republic of Lithuania	https://koronastop.lrv.lt/	EN, LT, RU, PL	Decentralized	Android® / iOS	ENS	Not clear		Entirely
PL	ProteGO Safe	Chief Sanitary Inspectorate	https://www.gov.pl/web/protegosafe	PL	Decentralized	Android® / iOS	ENS	Doc & Code		Entirely
SG	Trace Together	Ministry of Health	https://www.tracetogether.gov.sg/	EN	Centralized	Android® / iOS	BLUETRACE	Doc & Code		Partially

Country	Name	Promoter/health authority	Official site	Language	Approach	Os supported	Method	Transparency	PIA	Voluntary
ES	Radar COVID	Ministry of Health, Consumption and Social Welfare	https://radarcovid.gob.es/	ES	Decentralized	Android® / iOS	ENS	Doc & Code		Entirely
CH	SwissCovid	Federal Office of Public Health	https://foph-coronavirus.ch/swisscovid-app/	EN, DE, FR, IT	Decentralized	Android® / iOS	ENS	Doc & Code		Entirely
US	CoEpi	Community Epidemiology In Action project	https://www.coepi.org/	EN	Decentralized	Android® (beta) / iOS (beta + TestFlight)	TCN	Doc & Code		Entirely
NOTE 1: Android® is a trademark of Google LLC. NOTE 2: IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple under license.										

Main conclusions:

- A majority of initiatives have been promoted/supported, in some way, by public authorities, being CoEpi an exception as it is an initiative of the "Community Epidemiology in Action" project.
- A majority of the projects reviewed in the present document is in the decentralized paradigm space, with the exceptions of French "StopCovid" and Singaporean "TraceTogether". Beyond the fifteen apps studied here, Hungary's "VirusRadar", for instance, is an additional example of centralized solution within the European space.
- The preferred platforms are iOS and Android®. The availability of India's Aarogya Setu for KaiOS sounds to some extent anecdotic, as the fact that CoEpi is in a development stage (beta) with the need for TestFlight to run on iOS.
- The preferred digital contact tracing method is Google® & Apple® Exposure Notification System (ENS) API, despite the adoption of other relevant approaches, by some of the initiatives, like ROBERT, the proprietary approach of Aarogya Setu, PRONTO-C, BLUE TRACE and TCN.
- Transparency seems also paramount for most of the projects, despite only a couple of them have offered information about the Privacy Impact Analysis (PIA) performed by their domestic data protection authority.
- And, finally, with the only exception of Trace Together, almost the whole set of initiatives seems to show a voluntary spirit.

4.3.17 Other initiatives

The initiatives reviewed in clauses 4.3.1 to 4.3.15 above are not but a small selection of the whole universe of digital contact tracing apps (see [i.11], [i.12], [i.13] and [i.14]) that the COVID-19 pandemic has brought. Some sources (see [i.15], [i.16] and [i.17]) states that there are currently almost 10 times more contact tracing apps than the number explored in the present document (i.e. 120 apps available globally; of which India's Aarogya Setu is the most popular, with 100 million downloads, and where the US is the country with more apps, 23, than any other country in the world). Those same sources say that almost half that number of apps (48 %) use Bluetooth® as the primary contact tracing method and that more than one out of three (37,5 %) contact tracing apps are now using the Google® and Apple® ENS API.

All of that not to mention that there are many more apps scheduled to be rolled out nor the existence of other initiatives and proposals whose details are not publicly available.

Given this growing number of different initiatives it is not difficult to imagine that interoperability has become one of the most relevant challenges within the digital contact tracing space. That has been the very reason for establishing **ETSI's E4P Industry Specification Group** (see [i.18], [i.19], [i.20] and [i.21]) and it has also justified the effort by the European Commission to set up an EU-wide system to ensure interoperability (see [i.22]), the so-called **EU interoperability gateway**, recently gone live integrating, as a first step, the apps from Germany ("Corona-Warn-App"), Ireland ("COVID Tracker") and Italy ("Inmuni") (see [i.23]).

5 General approach to digital pandemic contact tracing

5.1 Generic systems using a back-end server, a mobile device & app, and Bluetooth® Low Energy

5.1.0 Overview

In general terms a digital pandemic contact tracing system aims at warning its users that they were in contact with individuals that may have been infected with a contagious disease (e.g. COVID-19). And in that sense, it is understood as a tool that supports manual contact tracing, making it more efficient.

In a high-level description of a digital contact tracing system (see [i.1]) the following essential elements can be distinguished:

- [End] **User**: a person that uses the digital contact tracing system through a *mobile device* and *app*.
- **Mobile Device**: an electronic device responsible for providing the proximity information, obtained via the *proximity detection method*, by communicating with other mobile devices and with an *infrastructure* through a *mobile application*.
- **Mobile Application** or '*app*': a piece of software running on the *mobile device*, responsible for registering and managing proximity information, communicating with the *infrastructure*, alerting the *end user* it may be infected (through a process called 'risk calculation') and notifying the central *infrastructure* in case the *end user* were tested positive.
- **Infrastructure** (i.e. back-end system/server): a set of technology elements (computers, databases, networks, …) that provides authoritative, trusted information to the *mobile device*. The main role of the *infrastructure* is to support information sharing between *users* through their *mobile devices* and *apps*. Should there were multiple *infrastructures* potentially using different *contact tracing protocols*, they might exchange information through a *federation protocol* to provide interoperability between the different digital contact tracing systems.
- **Proximity Detection Method**: the method used by *mobile devices* for detecting their proximity (based on Bluetooth® signals sent between devices) with potential sources of infection.
- **Contact Tracing Protocol**: the protocol between *mobile devices* and the *infrastructure*, used by the *mobile application*.

- **Federation Protocol**: a protocol used to exchange information between different *infrastructures*.
- **Health Authority**: the [usually public] authority overseeing the whole digital contact tracing system and process; and responsible for certifying the infection of a *user*.

This model describes the vast majority of digital contact tracing systems that are in use, or under development, at the time of writing the present document. These preliminary implementations of contact tracing protocols have been done mostly taking advantage of currently available "advanced" devices that already integrate all the necessary modules:

- a Bluetooth® Low Energy transceiver;
- a wireless communication capacity allowing IP connexions to public health infrastructure; and
- a CPU with memory for storage of ephemeral Bluetooth® Low Energy beacons and contacts logging.

Today all these capacities can be found in smartphones based on both, Apple® iOS and Google® Android operating systems.

5.1.1 Systems having possible risk of infection detected by a server

One of the current debates of contact tracing systems is about solutions having possible risk of infection detected by a server (**centralized approach**) or by a mobile device (**decentralized approach**) (see [i.24]).

In all systems (both centralized and decentralized) the digital pandemic contact tracing app of a certain user is regularly loaded with a list of ephemeral identifiers to be released in a given order. Each ephemeral identifier is repeatedly released during a certain interval. During such interval, the app instructs the mobile device to broadcast an ephemeral identifier frequently. At the same time, the app collects the ephemeral identifiers sent by a second user, which are received from her own app. Hence, the app of the first user manages two lists of identifiers: the ones to send (broadcast) and the received ones. Identifiers are stored with a time indication about when they have been sent/received. Quite regularly, very old identifiers are removed from their respective lists.

When a second user is tested positive, this diagnosed user receives from the health authority a token which allows her to upload information in a central server. This operation requires her consent, and she may have a control on what to upload.

Users can also check their "at-risk status". Essentially, with the help of the central server, they can figure out if they are at risk of being contaminated because they have met some person who were diagnosed.

In decentralized systems, risk calculation for a given user operates by having the user's app dump the content of the back-end server (i.e. the reported ephemeral identifiers from the list sent [to the back-end server] by the diagnosed user/-s) and check the intersection between the reported identifiers and the locally stored ones in her list of received ephemeral identifiers. Given the intersection of both lists, the app determines the at-risk status of the first user.

In centralized systems, ephemeral identifiers are derived from a pseudonym of the user, who has been previously registered in the back-end system. This latter, the central server, has a trapdoor allowing to retrieve the pseudonym from the identifier. Hence, the server can determine if a user, with a certain pseudonym, is at risk as soon as it recognizes said pseudonym from the received ephemeral identifier(-s). Hence, when the user's app connects to the server and authenticates under her pseudonym, the server can directly tell if the user is at risk.

In summary, the procedure for a centralized system is as follows:

- **Registration**. Each user's app registers to the server. The server sets a pseudonym. (The server and the app determine a way to authenticate the app under pseudonym through the anonymous channel).
- **Setup of identifiers**. Quite regularly, the app connects and authenticates to the server to get new identifiers. The server creates a list of ephemeral identifiers which can be mapped to app's pseudonym by using the back-end's trapdoor. The ephemeral identifiers are given to the app which stores them in a list (of to send ephemeral identifiers).
- **Broadcast**. During a given internal, the app constantly broadcasts an ephemeral identifier. Once this latter is broadcasted for the last time, it is erased from the to-send list. Every app from other users collects the broadcasted ephemeral identifier and stores it in a list of received ones together with a coarse time information.

- **Reporting**. Upon tested positive, a second, diagnosed user provides her own app with the appropriate (anonymous) credential to upload (part of) its list of received ephemeral identifiers to the back-end server. In this protocol, the first user's app does not authenticate to the server. Elements to report are sent separately to prevent the server from linking them. The server associates each reported ephemeral identifier with a pseudonym of the original (first) user in its database (using the trapdoor) and remembers that said pseudonym has to be notified.

- **Status verification**. Regularly, the first user's app connects and authenticates to the server to check the status of its user on the server. The server answers whether the user is at risk. If at risk, data about the pseudonym of that first user are erased and the user (her app) should register again.

5.1.2 Systems having possible risk of infection detected by a device

Decentralized systems work simpler, as follows (see [i.24]):

- **Setup of identifiers**. Quite regularly, a user's app prepares a list of random ephemeral identifiers to be used (broadcasted) and stores them in a list.

- **Broadcast**. During a certain interval of time, the user's app constantly broadcasts an ephemeral identifier. A few weeks after that ephemeral identifier is broadcasted for the last time, it is erased from the list of ephemeral identifiers of such user. Every other users' app collects the ephemeral identifier broadcasted by the first user and stores it in the other users' list of received ephemeral identifiers with some time information.

- **Reporting**. Upon tested positive, a second, diagnosed user provides her own app with the appropriate credential to upload (part of) her list of ephemeral identifiers to send (broadcast) to the back-end server. This latter publishes it.

- **Status verification**. Regularly, the app of the first user checks the newly uploaded ephemeral identifiers on the server and checks if they are element of her list of received ephemeral identifiers. This way, the user's app determines if she is at risk.

5.1.3 Commonalities and differences between systems

Commonalities between the different approaches to digital pandemic contact tracing systems, as the two detailed above, are numerous, starting with a shared core goal -save lives-, common technology (servers, smartphones, Bluetooth® Low Energy, etc.), overall architecture (mobile device, app, back-end system, etc.) or detailed functionalities (proximity detection, risk calculation, exposure notification, etc.). The **main difference** is that, depending on the approach, the at-risk status could be determined by the server (centralized approach) or the app (decentralized approach).

Beyond that, other differences are the following:

- *In centralized systems*, each user's app registers to the server in order to be provided with a pseudonym for the app/user.

- *In centralized systems*, the list of ephemeral identifiers to be broadcasted is obtained from a server. *In decentralized systems*, it is generated by the user's app itself.

- *In centralized systems*, what is uploaded is the list of received identifiers. *In decentralized systems*, what is uploaded is the list of used (broadcasted) identifiers.

5.2 Other systems

5.2.0 Overview

At the time of writing of the present document, digital pandemic contact tracing standardization efforts by ETSI ISG E4P focused mainly on the Bluetooth® Low Energy-fuelled smartphone apps domain. However, future steps could take also into account different approaches/technologies:

- tokens;

- acoustics;

- UWB;
- systems using elements communicating information from fixed locations (e.g. entrance of rooms, shops, buildings or other facilities);
- systems using elements communicating information linked to objects (e.g. via RFID tags);
- etc.

Depending on their adoption, such systems might be modelled in a future version of the present document. The present document briefly introduces some of them.

5.2.1 Token-based systems

As detailed in clause 4, above, a growing number of smartphone-based digital pandemic contact tracing apps have been, and are being, developed and are freely available on associated app portals. However, those systems suffer some drawbacks that limit their usage; for instance, to name a few:

- power drain;
- need to activate the app; and
- part of the population not easily covered:
  - people who do not have smartphones;
  - elderly people; or
  - people who are not allowed to use smartphones, like individuals in:
    - jails;
    - military facilities; or
    - protected industrial plants.

In parallel, other systems featuring different components, most notably token devices, have started to emerge (see [i.25]).

Contact tracing tokens (electronic devices with limited capacity for communication and/or computation) are an alternative to contact tracing [smartphone-based] apps. They are aimed at people who do not own or prefer not to use a cell phone. These devices are thought to be distributed, for instance, among vulnerable elderly people who have little or no family support or have mobility problems. Those tokens usually have unique QR codes and do not need charging as they have a battery life of up to nine months.

As in the case of smartphones, tokens could work by exchanging Bluetooth® signals with other nearby tokens or mobile phones that are running the related app. Users will be alerted by a contact tracing officer if they are detected to have been near someone infected with the coronavirus.

Data collected by the devices will be encrypted and kept in the token for a maximum of "n" days (n=25, in the case of Singapore (see [i.26]), where these tokens have already been deployed). Data cannot be accessed remotely as the tokens have no Internet nor cellular capabilities. Tokens have no Global Positioning System (GPS) connectivity, so they do not collect location data.

Despite having been, Singapore's TraceTogether tokens, the first solution of this nature promoted by a public health authority, some other initiatives can be mentioned, too:

- France's experiments with **StopCovid** and the Internet of things (see [i.27]);
- the European Institute of Innovation & Technology (**EIT**) proposal to develop anonymous COVID-19 contact tracing systems using physical tokens (see [i.28] and [i.29]) that received more than 60 expressions of interest to face concrete pilots;

- the **Simmel Project**, an open source, ballpen-shaped wearable platform that enables privacy-preserving contact tracing (see [i.30] and [i.31]). The platform is built around an RF52833 chip by Nordic Semiconductors and the project has explored two technology paths in parallel: Bluetooth® Low Energy and near ultrasound (NUS);

- the **Project Tracer** initiative, another completely open source project (see [i.32], [i.33], [i.34] and [i.35]) demonstrating the Google® & Apple® ENS API on microcontrollers (i.e. non-smartphone devices) having only Bluetooth® Low Energy and Wi-Fi® transceiver. The protocol is implemented on a generic ESP32 integrated circuit by Shanghai-based Espressif Systems. The project provides a small sized, low-power platform (device) which implements the aforementioned contact tracing standard;

- the **TraceSigma** initiative, an attempt by a group of Singaporean engineers, known as "Bettr", to complement smartphones as contact tracing solutions' devices (see [i.36], [i.37] and[i.38]). Project TraceSigma aims to develop and release open-sourced code and reference designs of a portable device to build and deploy compatible self-contained tracing devices. The project implements Singapore's OpenTrace/BlueTrace on an Espressif Systems's ESP32 microcontroller; or

- last but not least, **cercadti (TECHBOX)**: a Bluetooth®-based contact tracing solution presented in Spain by the firms Táctica Corporativa/Red Táctica and ADN Mobile Solutions as mentioned by the Spanish press (see [i.39] and [i.40]).

5.2.2 Acoustic-based systems

Despite the many benefits Bluetooth® technology provides, it has also the problem of traveling too far (e.g. through walls) reaching further than expected and, therefore, leading to a number of undesired false-positive close contacts. In this context, new research (see [i.41]) suggests that high frequency sounds passed between cell phones could be a way to more accurately trace the potential spread of the COVID-19 virus (i.e. do contact tracing).

The idea is **taking advantage of complementary [acoustic] sensors** and using them to detect proximity the same way current Bluetooth®-based protocols do; i.e. the system would generate random, anonymous IDs for each phone, automatically send ultrasonic signals -undetectable by humans- between microphones and speakers of phones within a certain radius, and use the information exchanged through this acoustic channel for contact tracing. If a person tested positive for COVID-19, she would update her anonymous IDs and the timestamp when the IDs were generated in the past two weeks to a central database managed by a trusted health care authority. Each individual in the system will pull the positive patient's IDs and compare locally to check whether she has had any contact with the patient.

Among the efforts to enable acoustic communications between devices that are equipped with microphones and speakers the following can be mentioned:

- **ACOUSTIC-TURF** (see [i.42] and [i. 3]), a privacy-preserving, automated contact tracing system to fight COVID-19 using acoustic signals sent from ubiquitous mobile devices. At a high level, ACOUSTIC-TURF adaptively broadcasts inaudible ultrasonic signals with randomly generated IDs in the vicinity. Simultaneously, the system receives other ultrasonic signals sent from nearby (e.g. 6 feet) users. In such a system, individual user IDs are not disclosed to others and the system can accurately detect encounters in physical proximity with 6-foot granularity. ACOUSTIC-TURF correctly determines that people on opposite sides of a wall are not in contact with one another;

- **Hush** (see [i.44]), a software that utilizes very high frequency sound to send data between commodity smart mobile devices;

- **U-Wear** (see [i.45]), a solution that enables data dissemination between ultrasonic wearable devices;

- **Dhwani** (see [i.46]), a work that employs audible sound for near field communications (NFC) between smartphones;

- **DopEnc** (see [i.47]), an initiative that can automatically identify persons with whom users interact and considers coordinating multiple access in order to measure the Doppler effect; or

- **NOVID** (see [i.48]), an attempt to integrate Bluetooth® and ultrasonic signals for distance-aware automated contact tracing.

Beyond the contact tracing space, another recent, early-staged, acoustic experimental approach, by MIT, (see [i.49]) is taking advantage of the changes infections usually cause on the quality of a patient's voice (e.g. lower volume, nasally tone), promising the future **use of mobile apps to screen people for a disease** (e.g. COVID-19), particularly those who are asymptomatic.

This **vocal screening for COVID-19** effort is based on the processing of speech recordings of people infected, but not yet showing symptoms; and has allowed to find evidence of measurable indicators (vocal biomarkers) of the disease. These biomarkers stem from disruptions the infection causes in the movement of muscles across the respiratory, laryngeal, and articulatory systems, all of them involved in speech production.

The initiative proposes (see [i.50]) a speech modelling and signal-processing framework to detect and track COVID-19 through asymptomatic and symptomatic stages. The approach is based on complexity of neuromotor coordination across speech subsystems involved in respiration, phonation and articulation.

6 Existing methods

6.1 Systems having possible risk of infection detected by a server

6.1.1 BlueTrace

Table 17: "BlueTrace" method characterization

Method's name	BlueTrace.
Specification (and source of this characterization) available at	https://bluetrace.io/ (official webpage) https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf ("BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders" whitepaper).
Description	BlueTrace is the protocol developed by the Singaporean Government for contact tracing of users to stem the spread of the COVID-19 pandemic. The BlueTrace protocol is a centralized one, with some particularities: • subscribers provide a phone number for urgent notification in case of positive contact detection. This allows to reach users even if the app is not on, or they have TraceTogether tokens; • there is a Bluetooth® Low Energy connected process in the protocol where the devices exchange complementary data in a file, containing the device's TempID, device model, health authority identifier, and BlueTrace protocol version; and, • the protocol allows devices with transmission only capabilities (for example, low power tokens). TraceTogether is the official mobile app integrating the BlueTrace protocol. OpenTrace is the open-source reference implementation of BlueTrace, used in the app and released under the GPL-3.0 license.
Device (front-end)	
Calibration method	
Server (back-end)	
Risk-calculation approach (on device/on server)	On server (centralized approach).
Epidemiological risk criteria	
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	The method has been promoted by the Government of Singapore through its Government Technology Agency and endorsed by the Singaporean Ministry of Health.
Degree of interoperability	
User experience & usability	
Impact on devices and data usage	

Privacy & security aspects	
Data anonymization/pseudonymization	
Data retention	
Proximity detection methods & technologies	Bluetooth® Low Energy.
Support of different device platforms	The TraceTogether app is available in both Apple App Store and Google Play. For TraceTogether tokens, there is a specific version of BlueTrace, called BlueTrace Light.

6.1.2 DESIRE

Table 18: "DESIRE" method characterization

Method's name	DESIRE.
Specification (and source of this characterization) available at	https://hal.inria.fr/hal-02570382/file/DESIRE-specification-EN-v1_0.pdf
Description	DESIRE is an evolution of ROBERT (see clause 6.1.3, below), leveraging the best of the so-called centralized and decentralized systems. DESIRE is based on Private Encounter Tokens (PET), generated from Ephemeral Bluetooth® Identifiers (EBID). The EBIDs and PETs are generated and computed locally by the mobile device and are non-linkable. A PET uniquely identifies an encounter between two devices and is secret (it can only be computed by the two devices). They can be generated from any Non-Interactive Key Exchange protocol, which makes them private and non-linkable from the server. For example, the creation of PET can be based on a Diffie-Hellman key exchange protocol (using an instance of the discrete logarithm on elliptic curves such as Curve25519). PET has the advantage over EBID that it reduces the ability of the server to link co-location information coming from different individuals. Furthermore, this method mitigates "replay attack", where a malicious individual collects the EBIDs received by an infected (or potentially infected) individual and replays them in many locations, thus creating a large number of false positives. Apps interact with the system through the following procedures: • Initialization: When a user wants to use the service, she installs the application (app) from an official and trusted app-store. The app then registers to the server, that generates a permanent identifier (ID). An IDTable keeps an entry for each registered ID. The stored information is "de-identified", i.e. by no mean, associated to a particular identity (no personal information is stored in the IDTable). • Proximity Discovery: After registering to the service, any given device 'A': – generates a new and non-linkable $EBID_A$ at each epoch; – broadcasts this $EBID_A$ regularly; – collects EBIDs of encountered devices; – generates PETs from collected EBIDs if certain conditions are satisfied on, for example, contact length, received signal strength, etc.; and – stores the generated PETs in a local list, along with, if necessary, additional metadata (contact length, speed, etc.). • Infected User Declaration: When an individual is tested and diagnosed COVID-positive, and after an explicit user consent and authorization (from the medical services), her smartphone's application uploads its local list of generated PETs (with the relevant metadata) to the authority server, that adds them in a global list, EList, of exposed PETs.

	• Exposure Status Request: The app queries -pull mechanism- the "exposure status" of its user by regularly probing the server with its list of generated PETs. The server then checks how many of the app's tokens appear in EList and computes a risk score from this information (and possibly other parameters, such as the exposure duration and signal strength). If this score is larger than a given threshold, the bit "1" ("at risk of exposure") is sent back to the app, otherwise the bit "0" is sent back. Upon reception of a message "1", a notification is displayed to the user that indicates the instructions to follow (e.g. go to the hospital for a test, call a specific phone number, stay in quarantine, etc.). This DESIRE protocol assumes that all the smartphones and the server are loosely time-synchronized (thanks to the Network Time Protocol, NTP) or any other time synchronization mechanism like cellular mobile phone network information, or GPS time information, etc.). Time is expressed as the NTP "Seconds" value, which represents, for era 0, the number of seconds since 0h January 1st, 1900 UTC. Time is discretised into epochs (e.g. of 15 minutes). epoch_duration_sec is the duration of an epoch in seconds. Epochs are synchronized with the (Bluetooth®) device address randomisation periods.
Device (front-end)	
Calibration method	Not part of DESIRE itself. Done by the mobile application.
Server (back-end)	
Risk-calculation approach (on device/on server)	On server (centralized approach), but DESIRE can be easily modified to be state-less with risk calculation done on the device.
Epidemiological risk criteria	As defined by health authorities.
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	Could be used in the next generation of the official French digital contact tracing application, StopCovid.
Degree of interoperability	
User experience & usability	Not applicable to a method/protocol.
Impact on devices and data usage	DESIRE uses Bluetooth® Low Energy and is thus dependent on the low level detail for energy consumption (its EBIDs are transmitted in 2 consecutive Bluetooth® packets). Data usage is mostly limited (bound by) the periodic probing of the server with the list of generated PETs.
Privacy & security aspects	DESIRE has been designed by researchers in the fields of security and privacy with major privacy improvements over ROBERT.
Data anonymization/pseudonymization	
Data retention	
Proximity detection methods & technologies	Bluetooth® Low Energy.
Support of different device platforms	As a protocol/method is largely independent of device platforms. DESIRE has been implemented and tested.

6.1.3 ROBERT

Table 19: "ROBERT" method characterization

Method's name	ROBERT (ROBust and privacy-presERving proximity Tracing protocol).
Specification (and source of this characterization) available at	https://hal.inria.fr/hal-02611265/document https://github.com/ROBERT-proximity-tracing/documents

Description	ROBERT assumes an ecosystem composed of users who install the proximity tracing application (app) and a back-end server (highly secured) under the control of the Health Authority. Apps interact with the system through the four following procedures: • Initialization: When a user wants to use the service, she installs the application (app) from an official app-store. The app then registers to the server that generates a permanent identifier (ID) and several Ephemeral Bluetooth® Identifiers (EBID). The back-end maintains a table, IDTable, that keeps an entry for each registered ID. The stored information is "anonymous" and, by no mean, associated to a particular user (no personal information is stored in the IDTable). • Proximity Discovery: After registering to the service, the app broadcasts HELLO messages over its Bluetooth® interface and collects HELLO messages from other devices, running the same application, in the vicinity. These HELLO's contain several fields, and in particular, an Ephemeral Bluetooth® Identifier. The collected HELLO messages are stored, together with the time of reception (and possibly other information such as the strength of the Bluetooth® signal or the user's speed) into a local list, the LocalProximityList. • Infected User Declaration: When an individual is tested and diagnosed COVID-positive, and after an explicit user consent and authorization (from the medical services), her smartphone's application uploads its LocalProximityList to the server that then flags as "exposed" all IDs of IDTable of which at least one EBID appears in the uploaded LocalProximityList. It is important to note that: – the server does not learn the identifiers of the infected user's app, but only the EBIDs contained in its LocalProximityList (list of Ephemeral Bluetooth® Identifiers she was in proximity with); and – given any two random identifiers of the IDTable that are flagged as "exposed", the server cannot tell whether they appeared in the same or in different LocalProximityList lists (the proximity links between identifiers are not kept and, therefore, no proximity graph can be built). • Exposure Status Request: The app queries -pull mechanism- the "exposure status" of its user by regularly probing the server with its EBIDs. The server then checks how many times the app's EBIDs were flagged as "exposed" and computes a risk score from this information (and possibly other parameters, such the exposure duration or the user's speed/acceleration during the contact). If this score is larger than a given threshold, the bit "1" ("at risk of exposure") is sent back to the app and her account is deactivated, otherwise the bit "0" is sent back. Upon reception of this message, a notification is displayed to the user that indicates the instructions to follow (e.g. go the hospital for a test, call a specific phone number, stay in quarantine, etc.). The ROBERT protocol assumes that all the smartphones and the server are loosely time-synchronized (thanks to the Network Time Protocol, NTP) or any other time synchronization mechanism like cellular mobile phone network information, or GPS time information, etc.). Time is expressed as the NTP "Seconds" value, which represents, for era 0, the number of seconds since 0h January 1st, 1900 UTC. Time is discretised into epochs (e.g. of 15 minutes). epoch_duration_sec is the duration of an epoch in seconds.
Device (front-end)	
Calibration method	Not part of ROBERT itself. Done by the mobile application (there is calibration in the StopCovid app).
Server (back-end)	
Risk-calculation approach (on device/on server)	On server (centralized approach).
Epidemiological risk criteria	As defined by health authorities.
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	Used in the official French digital contact tracing application, StopCovid.

Degree of interoperability	ROBERT was designed to be operated in several countries (it was the result of a collaboration between Fraunhofer AISEC in Germany and Inria in France).
User experience & usability	Not applicable to a method/protocol.
Impact on devices and data usage	ROBERT uses Bluetooth® Low Energy and is thus dependent on the low level detail for energy consumption. Data usage is mostly limited (bound by) the communication of LocalProximityList (see "Description" entry, above).
Privacy & security aspects	ROBERT has been designed by researchers in the fields of security and privacy.
Data anonymization/pseudonymization	
Data retention	
Proximity detection methods & technologies	Bluetooth® Low Energy.
Support of different device platforms	As a protocol/method it is largely independent of device platforms. It has been implemented in an application that is supported on both Android® and iOS (StopCovid).

6.2 Systems having possible risk of infection detected by a device

6.2.1 Contact Shield

Table 20: "Contact Shield" method characterization

Method's name	Contact Shield.
Specification (and source of this characterization) available at	https://developer.huawei.com/consumer/en/doc/Contact-Shield-V1/introduction-0000001050738511-V1
Description	Contact Shield is a basic COVID-19 contact tracing service for Huawei® smartphone users, provided by Huawei Mobile Services (HMS) Core, and based on Bluetooth® Low Energy and DP-3T open protocol. Government organizations or local public health authorities can authorize developers to develop COVID-19 contact tracing apps using Contact Shield APIs. By calling Contact Shield APIs, the app can access Contact Shield capabilities. COVID-19 contact tracing apps can interact with other devices while protecting user privacy to check whether a user has been in contact with a person tested positive for COVID-19. If so, the user will be notified and instructed to take relevant measures, effectively controlling the spread of the virus.

Device (front-end)	The key functions of Contact Shield are anonymous ID generation, Bluetooth® broadcasting and scanning, and exposure checking on device. The functionality split between the Contact Shield service and a contact tracing app is as follows: • Contact Shield: 1. Manage and store periodic keys, dynamically share codes, and derive, encrypt and decrypt keys. 2. Manage Bluetooth® broadcast and Bluetooth® data collection and storage. 3. Identify whether the user is a close contact. 4. Provide user authorization interaction interface at key control points such as service startup and periodic key upload. • Contact tracing app: 1. Enable or disable Bluetooth® broadcast and scanning. 2. Obtain the periodic key, key generation time, and initial key risk level from backend server. 3. When user is diagnosed, STB obtains the periodic key from HMS. 4. Set the frequency of downloading periodic key from backend server. 5. When a user becomes a close contact, a message is pushed.
Calibration method	GSMA TS.57 Bluetooth® Low Energy Calibration Testing.
Server (back-end)	
Risk-calculation approach (on device/on server)	On device (decentralized approach).
Epidemiological risk criteria	Defined by local public health authority. Contact Shield allows setting of time, distance and other criteria as required.
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	Contact Shield is available to the public health authorities for their COVID-19 contact tracing apps.
Degree of interoperability	
User experience & usability	
Impact on devices and data usage	
Privacy & security aspects	HMS Core Contact Shield does not run if the user has not installed any app that uses Contact Shield APIs. If the user uses such an app, HMS Core Contact Shield protects user privacy. Users can determine by themselves whether to enable Contact Shield, whether to upload anonymous identifiers to the cloud, and whether to obtain diagnosis results by themselves. Contact Shield's Software Development Kit does not collect any personal data. It only uses dynamically generated anonymous IDs to identity users and does not use any privacy information such as user locations and phone numbers. In addition, anonymous IDs on the cloud can be stored only for a limited period (for example, 14 days). After the user uninstalls an app using Contact Shield APIs, the user's historical data stored on the device will be deleted. The user can also manually delete all historical data. Only developers authorized by governments and strictly assessed by Huawei® can use Contact Shield APIs to develop apps. Huawei® will sign an additional service agreement stating the user privacy protection requirements with eligible developers who want to use Contact Shield APIs.
Data anonymization/pseudonymization	Contact Shield uses dynamically generated anonymous IDs to identity users and does not use any privacy information such as user locations and phone numbers. In addition, anonymous IDs on the cloud can be stored only for a limited period (for example, 14 days).
Data retention	After the user uninstalls an app using Contact Shield APIs, the user's historical data stored on the device will be deleted. The user can also manually delete all historical data.
Proximity detection methods & technologies	Bluetooth® Low Energy.

Support of different device platforms	Huawei® devices running HMS Core (APK) 4.1 or later support Contact Shield APIs. If a user, whose HMS Core (APK) version does not meet this requirement, uses an app developed based on Contact Shield APIs, the app will instruct the user to install the latest HMS Core (APK) version.

6.2.2 DP-3T

Table 21: "DP-3T" method characterization

Method's name	DP-3T (Decentralized Privacy-Preserving Proximity Tracing).
Specification (and source of this characterization) available at	https://raw.githubusercontent.com/DP-3T/documents/master/DP3T%20White%20Paper.pdf https://github.com/DP-3T
Description	Decentralized Privacy-Preserving Proximity Tracing (DP-3T) aspires to "minimize privacy and security risks for individuals and communities and guarantee the highest level of data protection" while performing contact tracing. The system has been deliberately designed to not support tracking positive cases, detect hotspots or trajectories of positive cases and sharing data for epidemiological research. The protocol is proposed to work on participating smartphones which locally generate pseudo-random ephemeral identifiers (EphIDs) and broadcast them using Bluetooth® Low Energy beacons. Simultaneously, the smartphones also listen for these beacons and store the broadcast EphIDs with a timestamp and signal attenuation to estimate exposure. The protocol also requires the support of an honest backend server that is available. The primary role of the server is to distribute anonymous exposure information to the apps of the participating devices. Further, the server is trusted to not add spurious exposure events or remove genuine exposure events. The backend is primarily present for aggregation and dissemination of information, all processing happens locally on the devices. The privacy of the users does not depend on the behaviour of the server. In the event of a positive infection diagnosis the user is authorized by the local health authorities to upload a protocol-specific representation of their EphIDs to the backend server for a time window during which they were contagious thus aiding decentralized proximity tracing. The authors also propose secure mechanisms to validate upload requests from personal devices. The backend server aggregates the uploaded EphID representations and distributes them to the participating devices when they query the server. Subsequently the devices can recompute the EphIDs of infected users locally. To facilitate masking the upload traffic of infected users the participating devices generate dummy traffic to provide plausible deniability of real uploads. If any recorded EphID matches those downloaded from the server then the user may have been exposed to the virus, the app estimates the exposure risk by looking at the exposure measurements of the matched beacons. In line with this framework three protocols are proposed with varying trade-offs between privacy and computation cost-Low-cost, Unlinkable and Hybrid. In the Low-cost variant the devices start by generating a random initial daily seed for the current day. The secret day seed is rotated daily, and the new seed is set as the hash of the previous day seed. The daily secret seed is used to generate a list of ephemeral ids with the lifetime of a few minutes, known as epoch (e.g. 15 minutes). If a user is diagnosed as infected, then they can send the secret seed along with the day corresponding to the first day of infection to the server. After this the phone deletes the secret seed and generates a new one and proceeds as before, this is done to prevent tracking. The server then disseminates the collected secret seeds and the day of infection to all the participating devices which in turn can compute the EphIDs from this information and check whether they have been exposed. If a match is observed, then the beacon's receive time and exposure measurement are taken into account for the exposure risk computation.

	The Unlinkable design improves upon Low-cost variant by offering better privacy properties at the cost of increased bandwidth. Instead of distributing the list of seeds of infected users, the backend server includes the hash of EphIDs in a Cuckoo filter which is then broadcast to the participating devices. A Cuckoo filter is a space-efficient probabilistic data structure which is used to test the set membership of an element. Due to the probabilistic nature a false positive is possible, however, a false negative is not. Using a Cuckoo filter precludes the adversaries from linking EphIDs of the infected users. It also allows the infected users to redact EphIDs corresponding to sensitive location or times. In this approach EphIDs are generated each epoch using a random per-epoch seed. In case of positive diagnosis the users upload a chosen set of EphIDs and corresponding epochs. The parameters of the Cuckoo Filter are chosen such that it produces about one false positive in a million users over a period of 5 years. Due to hashing of values before placing them in the Cuckoo filter and sparseness in a large set, enumeration attacks are not efficient, hashing also makes reversing the filter of limited use. The Hybrid design attempts to combine the benefits of both the previous approaches. In this approach the devices generate seeds for each time window (e.g. 2 hours) and then use the seeds to generate EphIDs as in the Low-cost approach. This allows better unlikability than the Low-cost design as well as the opportunity to redact EphIDs. However, the tracking protection is as not good as the Unlinkable design, though, the bandwidth cost is low.
Device (front-end)	The device is responsible for generating and transmitting EphIDs. It also needs to receive and store EphIDs from close by devices. In case of infection, the user needs to upload (distribute) artefacts, which allow other users to check, if they were in proximity of the device of the infected user. In case of the Low-cost variant these artefacts are the daily seeds. Any participant of the system needs to receive (download) the proximity detection artefacts provided by the infected users, e.g. the daily seeds. The device uses these artefacts and the EphIDs stored on the device to calculate an exposure risk.
Calibration method	
Server (back-end)	The backend acts as a technical mean for distributing the artefacts provided by the infected users to all participants in the system.
Risk-calculation approach (on device/on server)	On device (decentralized approach). The backend server aggregates the seeds (based on protocol chosen) of all infected users, and broadcasts them to all the users participating in exposure notification. The risk calculation itself happens on the device of the user.
Epidemiological risk criteria	The protocol estimates exposure risk of an individual by estimating the duration and proximity of exposure to an infected individual. The threshold parameter to initiate a notification can be tuned by the local health authority. The app computes an exposure score by aggregating all the matches in the last 14 days. The exposure measurement is based on the Bluetooth® signal attenuation, which provides a proxy for proximity, combined with the duration of exposure. If the exposure score is above the threshold then the user is notified and advised further.
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	DP-3T has been proposed by a group of security and privacy researchers from leading European universities as a secure and privacy-preserving system for proximity tracing at large scale. As per the description, all the expenses of the project have been funded from Prof. James Larus's discretionary funds at EPFL, in anticipation of a grant from the Botnar Foundation. The work of some of the researchers involved with the project has been funded by Google® in the past. No participants were funded by Apple®. This is important to mention as Google® and Apple® have proposed a COVID-19 tracking method with many similarities.

Degree of interoperability	The DP-3T protocols have been designed to interoperate with each other and all three variants support interoperability between different operators of different regions as long as one of the proposed variants is used. Additionally, the devices need to run all the protocols that they wish to interoperate with and the respective backend servers need to exchange data. The devices use the list of visited regions to fetch proximity tracing data broadcasted by that region's backend server for up to 14 days after the end of the users' visit. If a user is diagnosed as infected then the device uploads the data to the local backend server along with a list of visited regions. The local backend server in turn disseminates the data to all the visited regions so that everyone exposed can be notified. The protocol does not provide a way to interoperate with centralized protocols or other proximity tracing systems.
User experience & usability	The protocol requires minimal user interaction after the initial consent and setup. In the event of an infection the user needs to upload data (if they consent). Rest of the processes happens in the background. It should be noted that user experience depends to a large extent on the design of the app provided by the local health authority which utilizes the given protocol.
Impact on devices and data usage	Overall, the data requirements of all three variants of the protocol are not significant. Assuming a conservative estimate of 140 000 different observations, which would be 100 different people per 15 minute epoch the device storage required is below 7 MB. The backend server stores exposure related data for the last 14 days per individual, this is not significant. The data which is downloaded by the devices can be eased by using content delivery networks as it is static in nature. For all three protocol variants the daily data download size grows linearly with the number of infections. The authors provide an estimate of expected daily per user data download assuming a contagious window of 5 days and 15-minute epochs. During the peak of infection when some regions saw about 9 000 new cases daily the download amount for Low-cost, Unlinkable and Hybrid design was computed as 0,28 MB, 25,22 MB and 4,20 MB respectively. Considering, the size of some app updates this amount is not significant.
Privacy & security aspects	The DP-3T protocols have been designed with privacy in mind and they aim to ensure data minimization as the backend server only observes self-reported anonymous EphIDs of infected users without any proximity information. The protocol also reduces the scope of data abuse by limiting the backend server to receive only the information it needs. Tracking healthy users is not possible and limited for infected users. The design supports graceful dismantling, and the data is removed after 14 days from the app and the backend server. The protocols keep the social graph, interaction graph and location information of the individuals private. The users that receive an exposure notification are advised on subsequent steps to be taken but their identity is not revealed. Only a confirmed infected individual is reported to the authorities provided they consent. Also, no information regarding infection hotspots is collected.

	However, the protocols are not free from security and privacy weaknesses. The Low-cost design allows local tracking of users during the past window where the EphIDs are linkable. All decentralized proximity tracing systems suffer from exposing the identity of the person who might have exposed a user. More advanced attackers could also modify the app to record much more information than intended by the protocol, this could be mitigated by running the proximity tracing app withing a Trusted Execution Environment (TEE). Linking EphIDs with timing information can be used to narrow down the list of infected individuals, collation with other side-channels is also possible. Traffic masking is proposed to hide the communication with the backend server by using dummy traffic and batching. Further anonymity is proposed by precluding the backend from logging IPs. It is also suggested that the MAC address of the phone changes with EphID to prevent prolonged tracking. A resourceful adversary could potentially collect a large number of EphIDs using powerful antennas and then compare them with the list of infected EphIDs to track the movement of infected users in a small area for the Low-cost version of the protocol, thus isolating potential disease hotspots, the Unlinkable design makes this more challenging. To prevent an adversary from collecting large number of EphIDs a *k*-out-of-*n* secret sharing scheme is proposed where the EphIDs are broken into *n* chunks and at least *k* of them are needed to reconstruct an EphID fully, this could introduce an additional computational cost but would not limit a powerful adversary. The protocol could also be subject to security attacks such as fake exposure events by relaying or broadcasting EphIDs to large distances, suppressing at-risk contacts by tampering with the device local storage and preventing contact discovery by jamming Bluetooth® signals. The security and privacy risks listed here are non-exhaustive.
Data anonymization/pseudonymization	
Data retention	All received EphIDs are stored locally on the device apart from when an infection is reported, in which case the seeds/EphIDs are uploaded to the backend server.
Proximity detection methods & technologies	Bluetooth® Low Energy. The system uses Bluetooth® Low Energy and approximates the proximity using the Bluetooth® signal attenuation.
Support of different device platforms	The protocol places no limitation on the devices that it can be implemented on as long as they support Bluetooth® Low Energy beacons and have a modest computing power and storage capacity. So far, the popular choices have been implementation in the form of apps for Android® and iOS devices, but in the future they could also be implemented on tokens.

6.2.3 ENS

Table 22: "ENS" method characterization

Method's name	ENS (Exposure Notification System).
Specification (and source of this characterization) available at	https://www.Google.com/covid19/exposurenotifications/ (Google® site). https://developer.apple.com/exposure-notification/ (Apple® site).

Description	The Google & Apple® Exposure Notification System (ENS) is based on the ideas of DP-3T. The API was created with the vision that it would be widely used by COVID-19 contact tracing apps which would be developed independently by public health authorities. The API uses Bluetooth® Low Energy to detect proximity between people running the COVID-19 tracing apps. The users decide whether they wish to opt-in to the Exposure Notifications and the system does not collect any location information from the device. In the event of a positive infection diagnosis, it is up to the user to report this in the public health app. The service has been planned to be released in two phases: • first, in May 2020 the companies released APIs to enable interoperability between Android® and iOS devices using the apps from public health authorities; and • second, the companies would work on enabling a broader Bluetooth®-based contact tracing system by baking this functionality into the underlying operating systems. Close integration with the operating system would provide a more robust solution than the API and also simplify the participation of a broader section of apps and government health authorities. The information regarding the project details is planned to be published openly to facilitate transparency. The protocol works by exchanging randomised tokens between voluntarily participating devices which are running the same COVID-19 contact tracing app. The tokens, known as Rolling Proximity Identifiers (RPIs), are exchanged when the devices are in close proximity of each other. A 16-byte Temporary Exposure Key is generated locally on the device using cryptographic random number generator, the key is rotated every 24 hours. The Temporary Exposure Key is used to generate RPI Keys and Associated Encrypted Metadata (AEM) Keys. The AEM keys are used to encrypt the Bluetooth® metadata containing the transmit power level which is the measured radiated transmit power of Bluetooth® Advertisement packets and is used to improve distance approximation. RPIs are generated from RPI Keys and are rotated every 10-20 minutes (based on specification), the same frequency at which the Bluetooth® randomised address is changed, to prevent linkability and wireless tracking. Each participating device records a list of RPIs it encounters. In the event of an infection the device can choose to self-report the infection to a Diagnosis Server and upload a limited set of Temporary Exposure Keys known as Diagnosis Keys based on the time window of last 14 days. If the user remains healthy the Temporary Exposure Keys do not leave the device. The Diagnosis Server aggregates the Diagnosis Keys of all infected users, which are then broadcasted to all the devices participating in exposure notification, the participating devices download these keys at least once per day. The Diagnosis Keys are used to generate RPIs of infected users and matched locally on the device to the list of RPIs received. In the event of a match the user is notified and advised on the next steps. In the case of such a notification the system also shares the day the contact with the infected individual occurred, how long it lasted and the Bluetooth® signal strength of that contact.
Device (front-end)	The device has to generate all the necessary keys and the RPIs. It needs to send and receive RPIs. It needs to store received RPIs for a defined time window (currently 14 days). It needs to upload Diagnosis Keys in case of an infection. It has to download Diagnosis Keys of infected users from the backend. It has to calculate the risk score and, based on the risk score, inform people at risk.
Calibration method	
Server (back-end)	The backend server acts as a mean for implementing a broadcast of Diagnosis Keys to all participants in the system.
Risk-calculation approach (on device/on server)	On device (decentralized approach). The Diagnosis Server aggregates the Diagnosis Keys of all infected users and broadcasts them to all the users participating in exposure notification. The risk calculation itself happens on the device.
Epidemiological risk criteria	The service leaves the exact risk calculation of an exposure to the local public health authority. The APIs supports this by providing the apps an estimate of the time and distance of contact with an infected individual.

Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	Originally an initiative by Apple® and Google®, ENS has been proposed as a platform to enable COVID-19 contact tracing apps developed by public health authorities to work more accurately, reliably and effectively across both Android® phones and iPhones®. Today, a growing number of Governments are promoting/have promoted digital contact tracing projects based on the Apple®|Google® API.
Degree of interoperability	
User experience & usability	The system requires minimal user interaction after the initial consent and setup. In the event of an infection the user needs to upload the Diagnosis Keys (if they consent). Rest of the processes happens in the background. It should be noted that user experience depends to a large extent on the design of the app provided by the local health authority which utilizes the given API.
Impact on devices and data usage	The APIs incorporate a number of measures to reduce the energy and data impact of using such a system. It is recommended to set the Bluetooth® broadcasting interval to 200-270 milliseconds (subject to change). To maximize recording potential exposure events the scanning interval and window is planned to have sufficient coverage to discover nearby Exposure Notification Service advertisements within 5 minutes. The scanning strategy is further optimized by opportunistically leveraging existing wakes and scan windows and setting a minimum sampling period of 5 minutes. It is also envisioned to use Bluetooth® controller duplicate filters and other hardware filters to prevent excessive power drain. Further optimizations have also been implemented to improve performance such as using the Advanced Encryption Standard (AES) instead of HMAC<SHA256> for generating RPIs. The impact on data usage is not significant when only a few devices are in proximity but could be large in public spaces.
Privacy & security aspects	Since ENS follows a decentralized approach it inherits the security & privacy advantages and disadvantages associated with decentralized approaches. One advantage is, that there is not central entity which can easily learn even parts of the (pseudonymised) social graph. Disadvantages are, that one can learn who is infected and that disease hotspots can be detected by observing attackers. The Exposure Notification system is opt-in and the user can stop using it at any time. The infection reporting is also voluntary. To use the service user can download the app provided by the local health authority and activate the setting for COVID-19 notifications. This setting can be deactivated anytime subsequently. As a further safeguard the service can only be used in a health authority application, which need to satisfy specific criteria regarding data protection, security and data usage. The comparison of RPIs takes place completely on the device and the user identity is always kept private. Depending upon the locale, the health authority might require additional personal information such as age or gender while registering an individual as infected in their app. Providing such data is voluntary and is not shared with Google®, Apple® or other users. The advertiser address, RPI, and AEM are changed synchronously so that they cannot be linked. The Temporary Exposure Key schedule is fixed and mandated by the operating system components. This prevents the apps to track users by including static or predictable information. The 16-byte Temporary Exposure Keys make it computationally infeasible for an attacker to find a collision on a RPI, thus ruling out most of replay and impersonation attacks. The Diagnosis Server can purge metadata of clients uploading Diagnosis Keys after including those keys in the aggregated list of Diagnosis Keys per day. The Android® devices require activation of location detection to scan for Bluetooth® devices nearby but device location is not used for Exposure Notifications and is also explicitly excluded by the terms of use with the app provider, the service purely uses Bluetooth® beaconing for proximity detection. The service is planned to be disabled in future when it is no longer needed.
Data anonymization/pseudonymization	The RPIs can be considered to be transaction pseudonyms.
Data retention	All received tokens are stored locally on the device apart from when an infection is reported, in which case the Diagnosis Keys are uploaded to the Diagnosis Server.

Proximity detection methods & technologies	Bluetooth® Low Energy. The system uses Bluetooth® Low Energy and approximates the proximity using the radiated transmit power of Bluetooth® Advertisement packets.
Support of different device platforms	So far, the service has been designed to work on iOS and Android® operating systems. In future it may be possible to adapt the API to work with other devices such as tokens.
NOTE: An evolution of the Exposure Notification System (ENS), known as Exposure Notification Express (ENX) has been recently announced.	

6.2.4 IDPT/IDPT-FP

Table 23: "IDPT/IDPT-FP" method characterization

Method's name	IDPT/IDPT-FP (Interoperable Digital Proximity Tracing / Interoperable Digital Proximity Tracing-Full Protocol).
Specification (and source of this characterization) available at	https://github.com/IDPTdocs/documents
Description	The Interoperable Digital Proximity Tracing (IDPT) protocol can be run by applications that also run the DP-3T digital proximity tracking protocol to enable interoperability with the centralized digital proximity tracing protocols. The IDPT protocol avoids the re-identification attack of positive-tested users of the centralized system that was claimed to be an inherent property of interoperability systems, as in IDPT the system does not publish the list of decentralized ephemeral identifier that were at risk of exposure. Moreover, it avoids the possibility of creation of proximity graphs. IDPT-FP (Full Protocol) is a proposal for a digital proximity tracing protocol that can operate both in centralized and distributed mode with full interoperability. It is based on the mechanism described for the IDPT protocol.
Device (front-end)	In the case of IDPT, it transmits/receives DP-3T beacons and receives beacons from other centralized protocols. It transmits beacons carrying I-EBID information (32 bytes)
Calibration method	
Server (back-end)	Uses an I-relay, which publishes a list of values [(Hash(I-EBID^W, g^W, RSSI)]. This means that uses a Diffie-Heallman exchange to generate a shared secret between two devices that are in contact.
Risk-calculation approach (on device/on server)	On device (decentralized approach), though IDPT-FP can also work in centralized mode, i.e. on server.
Epidemiological risk criteria	
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	Secretaria de Estado de Digitalización e Inteligencia Digital (SEDIA), Spanish ministry "Ministerio de Asuntos Económicos y Transformación Digital".
Degree of interoperability	Allows interoperability between centralized and decentralized protocols.
User experience & usability	
Impact on devices and data usage	Potential increase of power consumption (in evaluation).
Privacy & security aspects	Allows interoperability without transferring vulnerability properties between centralized and decentralized protocols. In IDPT-FP avoids possibility of re-identify users, creation of social graphs and re-identification of infected users.
Data anonymization/pseudonymization	
Data retention	List of secret values X and received beacons for the last 14 days.
Proximity detection methods & technologies	Bluetooth® Low Energy (based on RSSI).
Support of different device platforms	It is independent of the operating system used.

6.2.5 [East Coast] PACT

Table 24: "[East Coast] PACT" method characterization

Method's name	PACT (Private Automated Contact Tracing).
Specification (and source of this characterization) available at	https://pact.mit.edu/ (official webpage). https://pact.mit.edu/wp-content/uploads/2020/05/PACT-Mission-and-Approach-2020-05-19-.pdf (PACT mission and approach). https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf ("The PACT Protocol Technical Specification").
Description	The Private Automated Contact Tracing protocol is a simple, decentralized approach to using smartphones for contact tracing based on Bluetooth® proximity. The PACT protocol broadcasts constantly-changing and randomly-chosen "chirp" values. When a user is tested and found positive, he becomes an "index case" in the traditional terminology. In the PACT system, an index case is strongly encouraged (but not required) to make public the chirp values he has broadcasted in the past three weeks, so that others may learn that they may have been exposed to the disease by being close to the index case. If someone learns that they have been so exposed, they may work with health authorities to determine the appropriate course of action.
Device (front-end)	
Calibration method	
Server (back-end)	
Risk-calculation approach (on device/on server)	On device (decentralized approach).
Epidemiological risk criteria	Those established by health authorities with respect to the "too close for too long" (TC4TL) principle; i.e. with respect to how to determine that two people have been closer than some medically relevant distance from each other for too long a period of time.
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	Promoters of, and contributors to, this method's specification have been a series of researchers (mainly from the Massachusetts Institute of Technology, among other entities) that have participated in their individual capacity and, therefore, without any kind of approval or commitment on behalf of any of the organizations involved. The goal of PACT is not to subsume medical professionals, but to give them the tools that they can use in their fight with disease. It is up to medical authorities to decide what to advise individuals to do based on the information they receive via the PACT app. Many factors may come into play in determining whether or not a user in possible risk of infection should be tested for disease - her symptoms, her risk factors, her location - her exposure risk score provided by PACT is just one of them. Any decisions for what the user should do from here should be done in consultation with doctors and health authorities. PACT serves as trusted technical advisor to US federal, state and local public health authorities.
Degree of interoperability	The PACT specification itself suggests the need for standardization in order to provide interoperability even between different implementations of this same method.
User experience & usability	
Impact on devices and data usage	
Privacy & security aspects	The privacy of the user is paramount in the PACT design. The PACT protocol satisfies the property that "no information, aside from the constantly-changing and randomly-chosen chirp values broadcasted, ever leaves the user's phone without his permission". The principles of voluntariness and consent underlay PACT's approach. Users of this scheme do not reveal anything about themselves unless they volunteer to do so. In particular, users can volunteer to donate their private data to a (trusted) health authority, who can then use this data to further control the spread of the virus, but this is discretionary to the users.
Data anonymiszation/pseudonymization	

Data retention	The chirps emitted to measure contacts are kept locally on each user's phone. Contact logs are kept for three months.
Proximity detection methods & technologies	Bluetooth® Low Energy.
Support of different device platforms	The PACT specification refers to the use of Apple® iOS "Find My" functionality as a natural extension to the protocol. With "Find My", each iPhone® device periodically broadcasts a 28-byte public key. This key changes randomly every 15 minutes to protect the privacy of the phone's owner. The idea would be just treating the public keys as if they were chirps. Additionally, the apps recently released by the US states of Delaware (COVID Alert DE), Pennsylvania (COVID Alert PA) and New York (COVID Alert NY) have been made available in both Apple® and Google® stores.

6.2.6 [West Coast] PACT

Table 25: "[West Coast] PACT"

Method's name	PACT (Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing).
Specification (and source of this characterization) available at	https://arxiv.org/pdf/2004.03544.pdf
Description	The Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing specification advocates for a third-party-free approach to assisted mobile contact tracing. The objective of PACT is to set forth transparent privacy and anonymity standards, which permit adoption of mobile contact tracing efforts while upholding civil liberties. PACT actually describes a series of mobile functionalities beyond digital contact tracing, as understood in the present document. Such functionalities seek to augment the services provided by public health authorities: • Mobile-assisted contact tracing interviews: a way to speed up manual contact tracing's interview processes by filling in [on a device] much of a contact interview form before the contact interview process even starts, reducing the burden on public health authorities. • Narrowcast messages: a capability that allows public health authorities to quickly warn specific, relevant subsets of citizens through custom-tailored messages (e.g. about extremely local pandemic-relevant events). • Privacy-sensitive, mobile tracing: an actual digital contact tracing protocol, as understood in the present document, based on the basic idea of having users broadcasting signals ("pseudonyms"), while also recording the signals they receive. A co-location approach that avoids the need to collect and share absolute location information. The mobile tracing approach offered by PACT relies on hash functions. Alternatively, it also offers an additional approach relying on signatures.
Device (front-end)	
Calibration method	
Server (back-end)	
Risk-calculation approach (on device/on server)	On device (decentralized approach).
Epidemiological risk criteria	Those established by health authorities with respect to the "too close for too long" (TC4TL) principle; i.e. with respect to how to determine that two people have been closer than some medically relevant distance from each other for too long a period of time.
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	Promoters of, and contributors to, this method have been a series of researchers (mainly from the University of Washington, among other entities). PACT has been designed with input from public health organizations.
Degree of interoperability	

User experience & usability	
Impact on devices and data usage	
Privacy & security aspects	PACT assumes that communication between device(-s) and server is protected using the Transport Layer Security (TLS) protocol. Privacy and integrity properties of the protocol follow two propositions: pseudo randomness and one-wayness.
Data anonymization/pseudonymization	
Data retention	
Proximity detection methods & technologies	Bluetooth® Low Energy.
Support of different device platforms	

6.2.7 Pronto-C2

Table 26: "Pronto-C2" method characterization

Method's name	Pronto-C2
Specification (and source of this characterization) available at	https://eprint.iacr.org/2020/493.pdf https://cryptoavengers.wordpress.com/home/pronto-c2/
Description	Pronto-C2 is a system composed by a smartphone application and a backend server that works mainly as a bulletin board. Pronto-C2 uses the following procedures: • Update Procedure: When a user wants to use the service, she installs the smartphone application. Each user that installs the smartphone application generates each day about 96 pairs (sk, pk) of secret and ephemeral keys. The expiration time of each of these pairs is 15 minutes. • Broadcast Procedure: The smartphone application broadcasts the current ephemeral key over the Bluetooth® interface. • Listen Event: The smartphone stores the ephemeral keys of other participants that are close enough together with the coarse time in which the meeting took place. • Test Positive Event: When a user tests positive for SARS-CoV-2, she will obtain from the health authority an activation code that will authorize the user to obtain a blind signature of the data to store on the server. The data to store on the server are computed as H(K||pkA||pkB) (we call this value "anonymous call"), where H is a collision-resistant hash function, (skA, pkA) are the pairs of keys used by the user 'A' in the last 14 days, pkB are the keys stored by 'A' in the last 14 days in the period in which pkA was broadcast and K is equal to pkB^skA. • Verification Procedure: Each user 'A' downloads the data from the server and checks that for all pairs (skA, pkA) used in the last 14 days and for all pkB stored in the last 14 days there are no data on the server equal to H(pkB^skA||pkB||pkA). If there is a match, 'A' receives an exposure notification. To minimize the exchanged data over the Bluetooth® interface, Pronto-C2 stores the ephemeral keys computed for the current day on a dedicated bulletin board. Every time that a user stores an ephemeral key on the bulletin board, she receives back the address in which the key is stored. In the Broadcast Procedure the user will broadcast the addresses of her ephemeral keys instead of using the ephemeral keys directly. Each user, at the end of the day, will download the ephemeral keys for all addresses collected during the day and then will proceed with the other steps of the protocol as previously described.
Device (front-end)	The device has to generate 96 pairs of secret and ephemeral keys per day. The device has to send the ephemeral keys to the bulletin board. The device has to broadcast and receive the addresses of the ephemeral keys. The device has to upload the anonymous calls to the server in case of an infection. The device has to download anonymous calls from the server. The device has to compute the risk score of the user.

Calibration method	n.a.
Server (back-end)	The backend server allows users to receive "calls" from infected users in order to be notified a risk; moreover, the backend server allows to download pseudonyms from the short addresses that are broadcasted via Bluetooth® Low Energy.
Risk-calculation approach (on device/on server)	On device (decentralized approach).
Epidemiological risk criteria	It is left to the local health authority.
Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	n.a.
Degree of interoperability	As many other contact tracing solutions, Pronto-C2 is not interoperable with other systems.
User experience & usability	All the operations can be computed in the background without requiring actions of the user. The user needs only to install the application and, in case of infection, the user will insert the code received by the health authority on the smartphone application.
Impact on devices and data usage	The intensive computation and data usage can be performed once a day while the smartphone is on charge and connected to a Wi-Fi network.
Privacy & security aspects	There is no central authority, the privacy of the user is guaranteed even if the user is infected. Pronto-C2 is resilient to several privacy and false security attacks.
Data anonymization/pseudonymization	Pronto-C2 broadcasts random identifiers that represent addresses of a bulletin board. The data stored on the bulletin board are ephemeral keys that are not linked to any user.
Data retention	The ephemeral keys and the anonymous calls are stored on two bulletin boards, while all the secret keys and the addresses are stored on the device.
Proximity detection methods & technologies	Bluetooth® Low Energy.
Support of different device platforms	The app is designed to work on Android® and could work on iOS if supported by Apple® . The system can be also implemented on hardware tokens. Obviously if Apple® and Google® make more generic their API for exposure notifications, then Pronto-C2 would be much more efficient.

6.2.8 TCN

Table 27: "TCN" method characterization

Method's name	TCN (Temporary Contact Numbers), formerly CEN (Contact Event Numbers).
Specification (and source of this characterization) available at	https://tcn-coalition.org https://github.com/TCNCoalition/TCN
Description	
Device (front-end)	
Calibration method	
Server (back-end)	
Risk-calculation approach (on device/on server)	On device (decentralized approach).
Epidemiological risk criteria	Those established by health authorities with respect to the "too close for too long" (TC4TL) principle; i.e. with respect to how to determine that two people have been closer than some medically relevant distance from each other for too long a period of time.

Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities	
Degree of interoperability	
User experience & usability	
Impact on devices and data usage	
Privacy & security aspects	TCN targets strong integrity, though initial implementations failed to fully achieve it.
Data anonymization/pseudonymization	
Data retention	
Proximity detection methods & technologies	Bluetooth® Low Energy.
Support of different device platforms	

7 Comparison of existing methods

7.1 Epidemiological risk criteria

Table 28: Comparative table of epidemiological risk criteria

Method	Epidemiological risk criteria
Blue Trace	n.a.
Contact Shield (Huawei®)	Defined by local public health authority. Contact Shield allows setting of time, distance and other criteria as required.
DESIRE	As defined by health authorities.
DP3T	The protocol estimates exposure risk of an individual by estimating the duration and proximity of exposure to an infected individual. The threshold parameter to initiate a notification can be tuned by the local health authority. The app computes an exposure score by aggregating all the matches in the last 14 days. The exposure measurement is based on the Bluetooth® signal attenuation, which provides a proxy for proximity, combined with the duration of exposure. If the exposure score is above the threshold then the user is notified and advised further.
ENS (Google® & Apple®)	The service leaves the exact risk calculation of an exposure to the local public health authority. The APIs supports this by providing the apps an estimate of the time and distance of contact with an infected individual.
IDPT/IDPT-FP	n.a.
[East Coast] PACT	Those established by health authorities with respect to the "too close for too long" (TC4TL) principle; i.e. with respect to how to determine that two people have been closer than some medically relevant distance from each other for too long a period of time.
[West Coast] PACT	Those established by health authorities with respect to the "too close for too long" (TC4TL) principle; i.e. with respect to how to determine that two people have been closer than some medically relevant distance from each other for too long a period of time.
Pronto-C2	It is left to the local health authority.
ROBERT	As defined by health authorities.
TCN	Those established by health authorities with respect to the "too close for too long" (TC4TL) principle; i.e. with respect to how to determine that two people have been closer than some medically relevant distance from each other for too long a period of time.

7.2 Promoters/Level of sponsorship, endorsement by, or involvement of, public health authorities

Table 29: Comparative table of promoters/level of sponsorship, endorsement by, or involvement of, public health authorities

Method	Promoters/level of sponsorship, endorsement by, or involvement of, public health authorities
Blue Trace	The method has been promoted by the Government of Singapore through its Government Technology Agency and endorsed by the Singaporean Ministry of Health.
Contact Shield (Huawei®)	Contact Shield is available to the public health authorities for their COVID-19 contact tracing apps.
DESIRE	Could be used in the next generation of the official French digital contact tracing application, StopCovid.
DP3T	DP-3T has been proposed by a group of security and privacy researchers from leading European universities as a secure and privacy-preserving system for proximity tracing at large scale. As per the description, all the expenses of the project have been funded from Prof. James Larus's discretionary funds at EPFL, in anticipation of a grant from the Botnar Foundation. The work of some of the researchers involved with the project has been funded by Google® in the past. No participants were funded by Apple®. This is important to mention as Google® and Apple® have proposed a COVID-19 tracking method with many similarities.
ENS (Google® & Apple®)	Originally an initiative by Apple® and Google®, ENS has been proposed as a platform to enable COVID-19 contact tracing apps developed by public health authorities to work more accurately, reliably and effectively across both Android® phones and iPhones®. Today, a growing number of Governments are promoting/have promoted digital contact tracing projects based on the Apple® |Google® API.
IDPT/IDPT-FP	Secretaria de Estado de Digitalización e Inteligencia Digital (SEDIA), Spanish ministry "Ministerio de Asuntos Económicos y Transformación Digital".
[East Coast] PACT	Promoters of, and contributors to, this method's specification have been a series of researchers (mainly from the Massachusetts Institute of Technology, among other entities) that have participated in their individual capacity and, therefore, without any kind of approval or commitment on behalf of any of the organizations involved. The goal of PACT is not to subsume medical professionals, but to give them the tools that they can use in their fight with disease. It is up to medical authorities to decide what to advise individuals to do based on the information they receive via the PACT app. Many factors may come into play in determining whether or not a user in possible risk of infection should be tested for disease - her symptoms, her risk factors, her location - her exposure risk score provided by PACT is just one of them. Any decisions for what the user should do from here should be done in consultation with doctors and health authorities. PACT serves as trusted technical advisor to US federal, state and local public health authorities.
[West Coast] PACT	Promoters of, and contributors to, this method have been a series of researchers (mainly from the University of Washington, among other entities). PACT has been designed with input from public health organizations.
Pronto-C2	n.a.
ROBERT	Used in the official French digital contact tracing application, StopCovid.
TCN	n.a.

7.3 Degree of interoperability

Table 30: Comparative table of degree of interoperability

Method	Degree of interoperability
Blue Trace	n.a.
Contact Shield (Huawei®	n.a.
DESIRE	n.a.
DP3T	The DP-3T protocols have been designed to interoperate with each other and all three variants support interoperability between different operators of different regions as long as one of the proposed variants is used. Additionally, the devices need to run all the protocols that they wish to interoperate with and the respective backend servers need to exchange data. The devices use the list of visited regions to fetch proximity tracing data broadcasted by that region's backend server for up to 14 days after the end of the users' visit. If a user is diagnosed as infected then the device uploads the data to the local backend server along with a list of visited regions. The local backend server in turn disseminates the data to all the visited regions so that everyone exposed can be notified. The protocol does not provide a way to interoperate with centralized protocols or other proximity tracing systems.
ENS (Google® & Apple®)	n.a.
IDPT/IDPT-FP	Allows interoperability between centralized and decentralized protocols.
[East Coast] PACT	The PACT specification itself suggests the need for standardization in order to provide interoperability even between different implementations of this same method.
[West Coast] PACT	n.a.
Pronto-C2	As many other contact tracing solutions, Pronto-C2 is not interoperable with other systems.
ROBERT	ROBERT was designed to be operated in several countries (it was the result of a collaboration between Fraunhofer AISEC in Germany and Inria in France).
TCN	n.a.

7.4 User experience and usability aspects

Table 31: Comparative table of user experience and usability aspects

Method	User experience and usability aspects
Blue Trace	n.a.
Contact Shield (Huawei)	n.a.
DESIRE	Not applicable to a method/protocol.
DP3T	The protocol requires minimal user interaction after the initial consent and setup. In the event of an infection the user needs to upload data (if they consent). Rest of the processes happens in the background. It should be noted that user experience depends to a large extent on the design of the app provided by the local health authority which utilizes the given protocol.
ENS (Google® & Apple®)	The system requires minimal user interaction after the initial consent and setup. In the event of an infection the user needs to upload the Diagnosis Keys (if they consent). Rest of the processes happens in the background. It should be noted that user experience depends to a large extent on the design of the app provided by the local health authority which utilizes the given API.
IDPT/IDPT-FP	n.a.
[East Coast] PACT	n.a.
[West Coast] PACT	n.a.

Pronto-C2	All the operations can be computed in the background without requiring actions of the user. The user needs only to install the application and, in case of infection, the user will insert the code received by the health authority on the smartphone application.
ROBERT	Not applicable to a method/protocol.
TCN	n.a.

7.5 Impact on devices and data usage

Table 32: Comparative table of impact on devices and data usage

Method	Impact on devices and data usage
Blue Trace	n.a.
Contact Shield (Huawei®)	n.a.
DESIRE	DESIRE uses Bluetooth® Low Energy and is thus dependent on the low level detail for energy consumption (its EBIDs are transmitted in 2 consecutive Bluetooth® packets). Data usage is mostly limited (bound by) the periodic probing of the server with the list of generated PETs.
DP3T	Overall, the data requirements of all three variants of the protocol are not significant. Assuming a conservative estimate of 140 000 different observations, which would be 100 different people per 15 minute epoch the device storage required is below 7 MB. The backend server stores exposure related data for the last 14 days per individual, this is not significant. The data which is downloaded by the devices can be eased by using content delivery networks as it is static in nature. For all three protocol variants the daily data download size grows linearly with the number of infections. The authors provide an estimate of expected daily per user data download assuming a contagious window of 5 days and 15-minute epochs. During the peak of infection when some regions saw about 9 000 new cases daily the download amount for Low-cost, Unlinkable and Hybrid design was computed as 0,28 MB, 25,22 MB and 4,20 MB respectively. Considering, the size of some app updates this amount is not significant.
ENS (Google® & Apple®)	The APIs incorporate a number of measures to reduce the energy and data impact of using such a system. It is recommended to set the Bluetooth® broadcasting interval to 200-270 milliseconds (subject to change). To maximize recording potential exposure events the scanning interval and window is planned to have sufficient coverage to discover nearby Exposure Notification Service advertisements within 5 minutes. The scanning strategy is further optimized by opportunistically leveraging existing wakes and scan windows and setting a minimum sampling period of 5 minutes. It is also envisioned to use Bluetooth® controller duplicate filters and other hardware filters to prevent excessive power drain. Further optimizations have also been implemented to improve performance such as using the Advanced Encryption Standard (AES) instead of HMAC<SHA256> for generating RPIs. The impact on data usage is not significant when only a few devices are in proximity but could be large in public spaces.
IDPT/IDPT-FP	Potential increase of power consumption (in evaluation).
[East Coast] PACT	n.a.
[West Coast] PACT	n.a.
Pronto-C2	The intensive computation and data usage can be performed once a day while the smartphone is on charge and connected to a Wi-Fi network.
ROBERT	ROBERT uses Bluetooth® Low Energy and is thus dependent on the low level detail for energy consumption. Data usage is mostly limited (bound by) the communication of LocalProximityList (see "Description" entry, above).
TCN	n.a.

7.6 Privacy & security aspects

Table 33: Comparative table of privacy & security aspects

Method	Privacy & security aspects
Blue Trace	n.a.
Contact Shield (Huawei®)	HMS Core Contact Shield does not run if the user has not installed any app that uses Contact Shield APIs. If the user uses such an app, HMS Core Contact Shield protects user privacy. Users can determine by themselves whether to enable Contact Shield, whether to upload anonymous identifiers to the cloud, and whether to obtain diagnosis results by themselves. Contact Shield's Software Development Kit does not collect any personal data. It only uses dynamically generated anonymous IDs to identity users and does not use any privacy information such as user locations and phone numbers. In addition, anonymous IDs on the cloud can be stored only for a limited period (for example, 14 days). After the user uninstalls an app using Contact Shield APIs, the user's historical data stored on the device will be deleted. The user can also manually delete all historical data. Only developers authorized by governments and strictly assessed by Huawei® can use Contact Shield APIs to develop apps. Huawei® will sign an additional service agreement stating the user privacy protection requirements with eligible developers who want to use Contact Shield APIs.
DESIRE	DESIRE has been designed by researchers in the fields of security and privacy with major privacy improvements over ROBERT.
DP3T	The DP-3T protocols have been designed with privacy in mind and they aim to ensure data minimization as the backend server only observes self-reported anonymous EphIDs of infected users without any proximity information. The protocol also reduces the scope of data abuse by limiting the backend server to receive only the information it needs. Tracking healthy users is not possible and limited for infected users. The design supports graceful dismantling, and the data is removed after 14 days from the app and the backend server. The protocols keep the social graph, interaction graph and location information of the individuals private. The users that receive an exposure notification are advised on subsequent steps to be taken but their identity is not revealed. Only a confirmed infected individual is reported to the authorities provided they consent. Also, no information regarding infection hotspots is collected. However, the protocols are not free from security and privacy weaknesses. The Low-cost design allows local tracking of users during the past window where the EphIDs are linkable. All decentralized proximity tracing systems suffer from exposing the identity of the person who might have exposed a user. More advanced attackers could also modify the app to record much more information than intended by the protocol, this could be mitigated by running the proximity tracing app withing a trusted execution environment (TEE). Linking EphIDs with timing information can be used to narrow down the list of infected individuals, collation with other side-channels is also possible. Traffic masking is proposed to hide the communication with the backend server by using dummy traffic and batching. Further anonymity is proposed by precluding the backend from logging IPs. It is also suggested that the MAC address of the phone changes with EphID to prevent prolonged tracking. A resourceful adversary could potentially collect a large number of EphIDs using powerful antennas and then compare them with the list of infected EphIDs to track the movement of infected users in a small area for the Low-cost version of the protocol, thus isolating potential disease hotspots, the Unlinkable design makes this more challenging. To prevent an adversary from collecting large number of EphIDs a *k*-out-of-*n* secret sharing scheme is proposed where the EphIDs are broken into *n* chunks and at least *k* of them are needed to reconstruct an EphID fully, this could introduce an additional computational cost but would not limit a powerful adversary.

	The protocol could also be subject to security attacks such as fake exposure events by relaying or broadcasting EphIDs to large distances, suppressing at-risk contacts by tampering with the device local storage and preventing contact discovery by jamming Bluetooth® signals. The security and privacy risks listed here are non-exhaustive.
ENS (Google® & Apple®)	Since ENS follows a decentralized approach it inherits the security & privacy advantages and disadvantages associated with decentralized approaches. One advantage is, that there is not central entity which can easily learn even parts of the (pseudonymised) social graph. Disadvantages are, that one can learn who is infected and that disease hotspots can be detected by observing attackers. The Exposure Notification system is opt-in and the user can stop using it at any time. The infection reporting is also voluntary. To use the service user downloads the app provided by the local health authority and activate the setting for COVID-19 notifications. This setting can be deactivated anytime subsequently. As a further safeguard the service can only be used in a health authority application, which need to satisfy specific criteria regarding data protection, security and data usage. The comparison of RPIs takes place completely on the device and the user identity is always kept private. Depending upon the locale, the health authority might require additional personal information such as age or gender while registering an individual as infected in their app. Providing such data is voluntary and is not shared with Google®, Apple® or other users. The advertiser address, RPI, and AEM are changed synchronously so that they cannot be linked. The Temporary Exposure Key schedule is fixed and mandated by the operating system components. This prevents the apps to track users by including static or predictable information. The 16-byte Temporary Exposure Keys make it computationally infeasible for an attacker to find a collision on a RPI, thus ruling out most of replay and impersonation attacks. The Diagnosis Server purges metadata of clients uploading Diagnosis Keys after including those keys in the aggregated list of Diagnosis Keys per day. The Android® devices require activation of location detection to scan for Bluetooth® devices nearby but device location is not used for Exposure Notifications and is also explicitly excluded by the terms of use with the app provider, the service purely uses Bluetooth® beaconing for proximity detection. The service is planned to be disabled in future when it is no longer needed.
IDPT/IDPT-FP	Allows interoperability without transferring vulnerability properties between centralized and decentralized protocols. In IDPT-FP avoids possibility of re-identify users, creation of social graphs and re-identification of infected users.
[East Coast] PACT	The privacy of the user is paramount in the PACT design. The PACT protocol satisfies the property that "no information, aside from the constantly-changing and randomly-chosen chirp values broadcasted, ever leaves the user's phone without his permission". The principles of voluntariness and consent underlay PACT's approach. Users of this scheme do not reveal anything about themselves unless they volunteer to do so. In particular, users can volunteer to donate their private data to a (trusted) health authority, who can then use this data to further control the spread of the virus, but this is discretionary to the users.
[West Coast] PACT	PACT assumes that communication between device(-s) and server is protected using the Transport Layer Security (TLS) protocol. Privacy and integrity properties of the protocol follow two propositions: pseudo randomness and one-wayness.
Pronto-C2	There is no central authority, the privacy of the user is guaranteed even if the user is infected. Pronto-C2 is resilient to several privacy and false security attacks.
ROBERT	ROBERT has been designed by researchers in the fields of security and privacy.
TCN	TCN targets strong integrity, though initial implementations failed to fully achieve it.

7.7 Data anonymisation/pseudonymisation

Table 34: Comparative table of data anonymisation/pseudonymisation

Method	Data anonymization/pseudonymization
Blue Trace	n.a.
Contact Shield (Huawei®)	Contact Shield uses dynamically generated anonymous IDs to identity users and does not use any privacy information such as user locations and phone numbers. In addition, anonymous IDs on the cloud can be stored only for a limited period (for example, 14 days).
DESIRE	n.a.
DP3T	n.a.
ENS (Google® & Apple®)	The RPIs can be considered to be transaction pseudonyms.
IDPT/IDPT-FP	n.a.
[East Coast] PACT	n.a.
[West Coast] PACT	n.a.
Pronto-C2	Pronto-C2 broadcasts random identifiers that represent addresses of a bulletin board. The data stored on the bulletin board are ephemeral keys that are not linked to any user.
ROBERT	n.a.
TCN	n.a.

7.8 Data retention

Table 35: Comparative table of data retention

Method	Data Retention
Blue Trace	n.a.
Contact Shield (Huawei®)	After the user uninstalls an app using Contact Shield APIs, the user's historical data stored on the device will be deleted. The user can also manually delete all historical data.
DESIRE	n.a.
DP3T	All received EphIDs are stored locally on the device apart from when an infection is reported, in which case the seeds/EphIDs are uploaded to the backend server.
ENS (Google® & Apple®)	All received tokens are stored locally on the device apart from when an infection is reported, in which case the Diagnosis Keys are uploaded to the Diagnosis Server.
IDPT/IDPT-FP	List of secret values X and received beacons for the last 14 days.
[East Coast] PACT	The chirps emitted to measure contacts are kept locally on each user's phone. Contact logs are kept for three months.
[West Coast] PACT	n.a.
Pronto-C2	The ephemeral keys and the anonymous calls are stored on two bulletin boards, while all the secret keys and the addresses are stored on the device.
ROBERT	n.a.
TCN	n.a.

7.9 Proximity detection method and technology

Table 36: Comparative table of proximity detection method and technology

Method	Proximity detection method and technology
Blue Trace	Bluetooth® Low Energy.
Contact Shield (Huawei®)	Bluetooth® Low Energy.
DESIRE	Bluetooth® Low Energy.
DP3T	Bluetooth® Low Energy. The system uses Bluetooth® Low Energy and approximates the proximity using the Bluetooth® signal attenuation.
ENS (Google® & Apple®)	Bluetooth® Low Energy. The system uses Bluetooth® Low Energy and approximates the proximity using the radiated transmit power of Bluetooth® Advertisement packets.
IDPT/IDPT-FP	Bluetooth® Low Energy (based on RSSI).
[East Coast] PACT	Bluetooth® Low Energy.
[West Coast] PACT	Bluetooth® Low Energy.
Pronto-C2	Based on Bluetooth® Low Energy.
ROBERT	Bluetooth® Low Energy.
TCN	Bluetooth® Low Energy.

7.10 Device platforms supported

Table 37: Comparative table of device platforms supported

Method	Device platforms supported
Blue Trace	The TraceTogether app is available in both Apple® App Store and Google Play. For TraceTogether tokens, there is a specific version of BlueTrace, called BlueTrace Light.
Contact Shield (Huawei®)	Huawei® devices running HMS Core (APK) 4.1 or later support Contact Shield APIs. If a user, whose HMS Core (APK) version does not meet this requirement, uses an app developed based on Contact Shield APIs, the app will instruct the user to install the latest HMS Core (APK) version.
DESIRE	As a protocol/method is largely independent of device platforms. DESIRE has been implemented and tested.
DP3T	The protocol places no limitation on the devices that it can be implemented on as long as they support Bluetooth® Low Energy beacons and have a modest computing power and storage capacity. So far, the popular choices have been implementation in the form of apps for Android® and iOS devices, but in the future they could also be implemented on tokens.
ENS (Google® & Apple®)	So far, the service has been designed to work on iOS and Android® operating systems. In future it may be possible to adapt the API to work with other devices such as tokens.
IDPT/IDPT-FP	It is independent of the operating system used.
[East Coast] PACT	The PACT specification refers to the use of Apple® iOS "Find My" functionality as a natural extension to the protocol. With "Find My", each iPhone® device periodically broadcasts a 28-byte public key. This key changes randomly every 15 minutes to protect the privacy of the phone's owner. The idea would be just treating the public keys as if they were chirps. Additionally, the apps recently released by the US states of Delaware (COVID Alert DE), Pennsylvania (COVID Alert PA) and New York (COVID Alert NY) have been made available in both Apple® and Google® stores.
[West Coast] PACT	n.a.
Pronto-C2	The app is designed to work on Android® and could work on iOS if supported by Apple® . The system can be also implemented on hardware tokens. Obviously if Apple® and Google® make more generic their API for exposure notifications, then Pronto-C2 would be much more efficient.

ROBERT	As a protocol/method it is largely independent of device platforms. It has been implemented in an application that is supported on both Android® and iOS (StopCovid).
TCN	n.a.

7.11 Summary

Apart from their different centralized/decentralized nature, in general terms, the contact tracing approach of the methods reviewed in the present document is quite similar. What really changes between them all -going to the details- is how the identifiers are generated or gathered (see [i.43]). The following table shows a summary of such differences.

Table 38: Summary table comparing reviewed digital contact tracing methods

Method	**Random Crypto Secrets Generation**				**Tracing Proximity measurement**	**Reporting Reported item**
	On device?	**Random secret (IDs)**	**# bits**	**Update frequency**		
Blue Trace	No	TempID	672	15 min.	Post-processing	TempIDs
Contact Shield (Huawei®)	Yes	n.a.	n.a.	n.a.	n.a.	n.a.
DESIRE	No	n.a.	n.a.	n.a.	n.a.	n.a.
DP3T	Yes	SK_t EphIDs	256 128	24 h. 1 min.	Threshold	SK_t, t
ENS (Google® & Apple®)	Yes	TEK RPIK RPI	128 128 128	24 h. 24 h. 15 min.	n.a.	TEK, t
IDPT/IDPT-FP	Yes	n.a.	n.a.	n.a.	n.a.	n.a.
[East Coast] PACT	Yes	Seed Chirp	256 224	1 h. n min.	n.a.	Seed, t
[West Coast] PACT	Yes	S_0 S_i ID_i	128 128 128	Infection period n h. n min.	Threshold	S_i, t
Pronto-C2	Yes	n.a.	n.a.	n.a.	n.a.	n.a.
ROBERT	No	ID EBID	40 64	Infection period 15 min.	n.a.	EBID, t
TCN	Yes	RAK, RVK TCK TCN	256 256 128	Infection period n h. 15 min.	Customized algorithm	RVK, TCK, t

NOTE: Adapted from [i.43], Table 1 (page 3). EphID: Ephemeral Identifier; SK: Secret Key; TCN: Temporary Contact Number; RAK: Report Authorization Key; TCK: Temporary Contact Key; RVK: Report Verification Key; TEK: Temporary Exposure Key; RPIK: Rolling Proximity Identifier Key; EBID: Ephemeral Bluetooth® Identifier.

An additional point to emphasize is that, with this large number of emerging solutions, it is often difficult to interpret what "privacy preserving" means in many of these protocols (e.g. not in all cases a privacy impact assessment has been available; the job done by Irish or German data protection authorities regarding their national apps -as implementation of these methods- is worth the mention).

Finally, convergence between this disparity of systems should favor greater interoperability, resulting in less confusion about alternatives, wider adoption, and, at the end, greater medical utility.

8 General challenges of digital pandemic contact tracing solutions

8.1 Readiness: overall pandemic mitigation and containment mechanisms

Despite being an invaluable resource in the fight against a pandemic, **digital contact tracing solutions are**, in themselves, no other thing that **a mere component of an overall healthcare effort**. Having the finest, user-friendliest, most innovative app means not necessarily success in interrupting ongoing transmission and in reducing the spread of an infection.

A series of factors, both contextual, behavioral, legal and technical, among others, may impact the success (i.e. the effectiveness) of any digitally-reinforced contact tracing initiative.

During a pandemic, digital contact tracing efforts lay over a more general set of healthcare mechanisms (context) established by Government and, particularly, Public Health Authorities.

The coordination of a region/nation-wide response to identify and isolate infected individuals requires acting early, quickly and decisively. Such an agile response, of which contact tracing -both traditional and digital- are core components, may benefit greatly from the lessons learned in previous pandemics. At the same time, it can become unfruitful should **the right mechanisms are not in place** (e.g. availability of trained and aware personnel -particularly at primary care centers-, availability of Personal Protection Equipment for healthcare professionals, massive use of face masks, physical distancing, [self-]isolation, travel restrictions, and, specially, widespread testing and rapid results).

8.2 Adoption

Weighting the success of an app by measuring its level of adoption is a common practice in any app's deployment. Measuring take-up rates when it comes to digital contact tracing results paramount in terms of effectiveness of the overall solution/process.

That said, there are a number of issues that may prevent adoption rates to scale:

a) **unavailability of appropriate devices** (in some regions or segments of population);

b) **unawareness on the existence of the app** (due to insufficient publicity);

c) mere **unavailability of the app** (due to restrictions imposed by app-stores before certain potentially malicious pieces of software);

d) **lack of tech-savvy citizenship** (e.g. elder people; minorities or vulnerable collectives in risk of financial/social exclusion);

e) **lack of transparency**;

f) **lack of trust** (negative perception by citizenship); etc.

Any improvement in this regard -even in the apps themselves (e.g. by **including a "Share this app" functionality as a UI/UX requirement**)-, would benefit adoption rates (for instance, contributing to spread the use of an app by inviting family and friends to use it).

The voluntary nature of a majority of these apps makes also relevant **the need for some pedagogy, clarity and fluent communication by pandemic-savvy authorities**, as well as the **engagement of civil society** in this joint public-private effort, in order to counteract a low number of downloads/installations/set-ups/log-in's, a relevant number of de-installations (once an app has been downloaded) and a low number of positive testing notifications and/or self-isolations. These last circumstances being able to benefit, also, from proper **economic incentives**.

8.3 Effectiveness

As pointed out above, the **adoption rate** of an app is one of the factors impacting directly on the effectiveness of digital contact tracing initiatives: the more take-up, the more efficacy! **Technical functioning** is the other one, and has to do with the lack of accuracy of Bluetooth®.

Using Bluetooth® technology to determine proximity can yield to **false positives** (e.g. two people in adjacent rooms or other two being even at 10-20 metres distance are reported to be together) and, therefore, to recommend unnecessary isolation, in case a recent "contact" tests positive.

At the same time, Bluetooth® can also yield to **false negatives**, i.e. undetected positives, leading to misleading warnings (e.g. "No risk of infection!").

8.4 Asynchronous contact tracing

The case of false negatives posed in clause 8.3 above, closely relates with the inability of current digital contact tracing solutions to detect that a user has entered a possibly-infected space that an infected person has just left; or that that same user has touched a surface or object that a contagious individual has recently "infected".

This sort of **indirect infection person-object-person** (**or direct person-to-person**) **when the two persons are not in the infectious place at the same time** represents an actual challenge for current digital "synchronous" contact tracing systems. It requires a new **asynchronous contact tracing** approach.

The [East Coast] PACT method already mentioned in the present document is an example of protocol whose specification contemplates an extension that allows for contact tracing when the virus is transmitted through fomite (surface) transmissions.

8.5 Ethics

As pointed out above, the adoption, use and, therefore, effectiveness of digital contact tracing systems may be impacted by a set of different factors, being **Ethics** not the least relevant. Issues regarding **the surveillance of citizens' behavior by central governments, democracy, freedoms, algorithmic bias, stigmatization, marginalization, discrimination, abuse and even the environment** -privacy will be treated in clause 8.6, below- are all concerns of the first magnitude that may discourage people from taking-up such solutions and their related procedures.

The goal of digital contact tracing needs to be balanced with the **maintenance of trust**. The **possible loss of liberties** should be only temporary, i.e. it **should not go beyond the crisis/pandemic**, preventing them to be normalized and extended indefinitely in the society.

Oversight by all relevant stakeholders, based on **well-known ethical principles** (respect, fairness, etc.), and the **availability of** a technically auditable solution (**source code**), is a guarantee of transparency of the whole process.

Finally, **information sharing** with other countries, particularly the most disadvantaged ones, has to be also part of any digital contact tracing initiative's moral duties and ultimate goal, i.e. to reduce suffering.

8.6 Privacy

When it comes to the use of digital solutions (e.g. smartphone apps), it is common for the average user to provide their personal data in exchange for any consideration in the form of a service. However, the situation often changes radically when such data transmission is carried out at the request of a public body, as it could be the case of digital contact tracing systems. In this case, the main problem regards to the type of information which is collected from each person and the way related data is treated by companies and institutions. Concerns about the **privacy of the medical data** being gathered, then, arise.

Therefore, as with other ethical issues, privacy requires that digital contact tracing initiatives count with some kind of **independent oversight** by all relevant stakeholders (including authorities as well as affected groups of citizens), in order to ensure data will not be used for purposes other than those related to the fight against a pandemic. In that sense, a **privacy impact analysis** by a regulatory body can become the best way to check the effectiveness of both, **privacy-by-design** as well as **privacy-by-default** development approaches.

In summary, the preservation of:

a) transparency regarding the use of gathered data;

b) each citizen's individual privacy; and

c) the voluntary nature (consent) of digital contact tracing solutions (despite the impact of voluntary adoption on their efficacy) are all unavoidable conditions for any governmental digital contact tracing effort to be lawful and, at the same time, proportionate.

8.7 Digital fragility

Digital permeates the whole society in all its aspects and will continue doing so. Fragility, unfortunately, permeates all things digital and mobile device-based contact tracing is no exception.

The increasing degree of digital dependency makes it evident, too, a growing level of **digital fragility**, i.e. that of digital nature, whose more usual expression adopts the form of **weak security** (or cybersecurity).

A number of **digital risks**, from **software glitch, error, negligence, misuse or fraud to even sabotage** during the development, deployment and operation/use stages of Government-sponsored digital contact tracing systems will be threatening the feasibility of any of these counter-pandemic solutions.

Once more time, **rigor in awareness, training, processes** and the availability of these systems' source code (that will allow to audit all their details in the area of cybersecurity, as it should be done regarding trust, ethics, privacy, etc.) will contribute to minimize digital contact tracing's cyber-fragility.

Security, as data anonymization, has to be demonstrated by evidence. And, in no case, should it [security] be belittled in favor of privacy.

8.8 Interoperability

Globalization and permanent mobility explain the ultimate challenge of digital contact tracing systems: interoperability.

A common trait of the whole "universe of apps" referenced in this technical report is their **inability to interoperate**. That has been the very *raison d'être* of E4P and it is the issue on which the most attention is being paid by this industry specification group.

But, indeed, it is not only an issue between apps/countries; i.e. when, within a given country, its Health system is decentralized, the "national" app could have to interact with several regional/local back-end systems, or, in other case, there will be several apps replicating the international interoperability issue at a domestic level.

Annex A: Bibliography

Abedi, Naeim; Ashish Bhaskar and Edward Chung: "Bluetooth® and Wi-Fi MAC Address Based Crowd Data Collection and Monitoring: Benefits, Challenges and Enhancement". 36th Australasian Transport Research Forum (ATRF) 2013 Proceedings. Brisbane, Australia. October 2-4, 2013.

NOTE: Available at https://www.researchgate.net/publication/259900889_Bluetooth®_and_Wi-Fi_MAC_Address_Based_Crowd_Data_Collection_and_Monitoring_Benefits_Challenges_and_Enhancement.

Ada Lovelace Institute: "Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis". Ada Lovelace Institute. Rapid evidence review. April 20, 2020.

NOTE: Available at https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf.

AEPD: "AEPD's notice on Coronavirus self-assessment apps and websites". Spanish Data Protection Agency, AEPD. March 26, 2020.

NOTE: Available at https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/aepds-notice-on-coronavirus-self-assessment-apps-and-websites.

Aguiar Alberto R.: "Radar COVID ya está rastreando contactos en España: así han ayudado o fracasado las apps de 5 países europeos combatiendo los rebrotes de coronavirus". Business Insider Spain. August 27, 2020.

NOTE: Available at https://www.businessinsider.es/resultados-5-apps-europeas-rastrear-contactos-como-radarcovid-704325.

Aguiar Alberto R.: "La peor noticia para las apps que rastrean contactos del coronavirus: no hay método infalible para calcular si son útiles". Business Insider Spain. September 12, 2020.

NOTE: Available at https://www.businessinsider.es/eficacia-apps-rastreo-contactos-no-puede-demostrar-715641.

Aguiar Alberto R.: "El caos de los códigos para notificar positivos en la app de rastreo del coronavirus cuestiona la efectividad de Radar COVID un mes después de su puesta en marcha". Business Insider Spain. September 21, 2020.

NOTE: Available at https://www.businessinsider.es/caos-codigos-notificar-positivos-app-rastreo-coronavirus-721525.

Asher Saira: "Coronavirus: Why Singapore turned to wearable contact-tracing tech". BBC.com. July 5, 2020.

NOTE: Available at https://www.bbc.com/news/technology-53146360.

Babones Salvatore: "Countries Rolling Out Coronavirus Tracking Apps Show Why They Can't Work". Foreign Policy. May 12, 2020.

NOTE: Available at https://foreignpolicy.com/2020/05/12/coronavirus-tracking-tracing-apps-cant-work-south-korea-singapore-australia/.

Beaudouin-Lafon Michel, Enrico Nardelli, Gerhard Schimpf, Panagiota Fatourou, Mario Fritz, Fabrizio Gagliardi, Oliver Grau and Chris Hankin: "Statement on essential principles and practices for COVID-19 contact tracing applications". The Association for Computing Machinery, ACM. May 5, 2020.

NOTE: Available at https://www.acm.org/binaries/content/assets/public-policy/europe-tpc-contact-tracing-statement.pdf.

Bergen Peter: "The disease expert who warned us". CNN.com. March 11, 2020.

NOTE: Available at https://edition.cnn.com/2020/03/10/opinions/osterholm-coronavirus-interview-bergen/index.html.

Bergen Peter: "Infectious disease expert: We're only in the second inning of the pandemic". CNN.com. April 22, 2020.

NOTE: Available at https://edition.cnn.com/2020/04/21/opinions/bergen-osterholm-interview-two-opinion/index.html.

Beskorovajnov Wasilij, Felix Dörre, Gunnar Hartung, Alexander Koch, Jörn Müller-Quade and Thorsten Strufe: "ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy". May 6, 2020.

NOTE: Available at https://eprint.iacr.org/2020/505.pdf.

Bluetooth® SGI: "Core Specifications". Bluetooth® SGI. December 31, 2019.

NOTE: Available at https://www.bluetooth®.com/specifications/bluetooth®-core-specification/.

BSI PAS 277:2015: "Health and wellness apps - Quality criteria across the life cycle - Code of practice". The British Standards Institution. April, 2015.

NOTE: Available at https://shop.bsigroup.com/upload/271432/PAS%20277%20(2015)bookmarked.pdf.

Byford Sam: "Japan rolls out Microsoft-developed COVID-19 contact tracing app". The Verge. June 19, 2020.

NOTE: Available at https://www.theverge.com/2020/6/19/21296603/japan-covid-19-contact-tracking-app-cocoa-released.

Cadzow Scott and Suno Wood: "The role of SDOs in developing standards for ICT to mitigate the impact of a pandemic". ETSI White paper no. 33, 1st edition. May, 2020.

NOTE: Available at https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp33_eHealth_standard_role_pandemic.pdf.

Canca Cansu: "Why 'Mandatory Privacy-Preserving Digital Contact Tracing' is the Ethical Measure against COVID-19". Medium.com. April 10, 2020.

NOTE: Available at https://medium.com/@cansucanca/why-mandatory-privacy-preserving-digital-contact-tracing-is-the-ethical-measure-against-covid-19-a0d143b7c3b6.

Carrión Francisco: "Las aplicaciones móviles contra el coronavirus más (y menos) invasivas del mundo". ElMundo. June 24, 2020.

NOTE: Available at https://www.elmundo.es/internacional/2020/06/24/5ef3870efdddff1a298b456e.html.

Castillo Carlos del: "Cinco claves de la tecnología de rastreo de contactos explicadas por sus creadores: 'Funciona como un submarino'". ElDiario.es/Tecnología. May 10, 2020.

NOTE: Available at https://www.eldiario.es/tecnologia/tecnologia-rastreo-contactos-cuestion-politica_1_5957403.html.

Castillo Carlos del: "El Gobierno libera el código de Radar COVID para mostrar cómo funciona, como pedían académicos y expertos". ElDiario.es/Tecnología. September 8, 2020.

NOTE: Available at https://www.eldiario.es/tecnologia/gobierno-libera-codigo-radar-covid-mostrar-funciona-solicitarlo-academicos-expertos_1_6207478.html.

CC4DR: "Declaration of Cities Coalition for Digital Rights". Cities Coalition for Digital Rights, CC4DR. CitiesForDigitalRights.org.

NOTE: Available at https://citiesfordigitalrights.org/assets/Declaration_Cities_for_Digital_Rights.pdf.

CC4DR: "Global coalition of cities for digital rights announces 10 principles for the responsible use of technologies during COVID-19 response". Cities Coalition for Digital Rights, CC4DR. CitiesForDigitalRights.org. Press release. June 3, 2020.

NOTE: Available at https://citiesfordigitalrights.org/sites/default/files/CC4DR%20COVID-19%20Digital%20Tech%20Statement%20Press%20Release_final%20...%20%281%29_0.pdf.

CCI: "COVID-19 Credentials Initiative". COVID-19 Credentials Initiative, CCI.

NOTE: Available at https://www.covidcreds.com/.

CDC: "Preliminary Criteria for the Evaluation of Digital Contact Tracing Tools for COVID-19". Centers for Disease Control and Prevention. May 17, 2020.

NOTE: Available at https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/prelim-eval-criteria-digital-contact-tracing.pdf.

CDC: "Digital Contact Tracing Tools". Centers for Disease Control and Prevention. May 26, 2020.

NOTE: Available at https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/digital-contact-tracing-tools.html.

CDC: "Contact Tracing: Using Digital Tools". Centers for Disease Control and Prevention. October 10, 2020.

NOTE: Available at https://www.cdc.gov/coronavirus/2019-ncov/downloads/digital-contact-tracing.pdf.

CDC: "Case Investigation and Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic". Centers for Disease Control and Prevention. October 21, 2020.

NOTE: Available at https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html.

Chen Lanhee J.: "The US has a lot to learn from Taiwan's Covid fight". CNN.com. July 10, 2020.

NOTE: Available at https://edition.cnn.com/2020/07/10/opinions/taiwan-covid-19-lesson-united-states-chen/index.html.

Cho Hyunghoon, Daphne Ippolito and Yun William Yu: "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs". arXiv:2003.11511v2 [cs.CR]. March 30, 2020.

NOTE: Available at https://arxiv.org/abs/2003.11511.

Chua Ming Hui, Weiren Cheng, Shermin Simin Goh, Junhua Kong, Bing Li, Jason Y. C. Lim, Lu Mao, Suxi Wang, Kun Xue, Le Yang, Enyi Ye, Kangyi Zhang, Wun Chet Davy Cheong, Beng Hoon Tan, Zibiao Li, Ban Hock Tan, and Xian Jun Loh: "Face Masks in the New COVID-19 Normal: Materials, Testing, and Perspectives". Research, Volume 2020, Article ID 7286735. August 7, 2020.

NOTE 1: Available at https://doi.org/10.34133/2020/7286735.

NOTE 2: Available at http://downloads.spj.sciencemag.org/research/2020/7286735.pdf.

CODE4JAPAN: "mamori-i-japan project repository ". GitHub.

NOTE: Available at https://github.com/mamori-i-japan.

Collins Katie: "Europe develops coronavirus tracking app meant to also preserve privacy". C|Net.com. April 10, 2020.

NOTE: Available at https://www.cnet.com/news/europe-develops-coronavirus-tracking-app-meant-to-also-preserve-privacy/.

COVID-19 MLIA: "Covid-19 MLIA Eval". COVID-19 MultiLingual Information Access, MLIA.

NOTE: Available at http://eval.covid19-mlia.eu/.

COVID WATCH: "COVID Watch app official website".

NOTE: Available at https://www.covidwatch.org/.

COVID WATCH: "COVID Watch: Bluetooth® contact tracing functionality" (video).

Criado Arturo: "La app de rastreo del Covid-19 podría quedarse en el cajón tras las experiencias europeas". El Español/Invertia. July 28, 2020.

NOTE: Available at https://www.elespanol.com/invertia/observatorios/digital/20200728/rastreo-covid-19-podria-quedarse-cajon-experiencias-europeas/508450265_0.html.

Cross Sean: "Trace Together Token: Teardown and Design Overview". Xobs.io. June 21, 2020.

NOTE: Available at https://xobs.io/trace-together-token-teardown/.

Decentralized ID: "Rebooting Web Of Trust - Papers and Advance Readings Index". July 7, 2019.

NOTE: Available at https://decentralized-id.com/literature/rebooting-web-of-trust/.

Deloitte: "What do businesses need to overcome the pandemic? Rebuilding trust with blockchain technology".

NOTE: Available at https://www2.deloitte.com/be/en/pages/tax/articles/covid-19_rebuilding-trust-with-blockchain-technology.html?_lrsc=f1526a08-0c1a-4c4f-9c4c-26bc5f262c64&id=wl:2sm:3li:4elevate:5awa:6oth:274530:1033477.

Devteam.Space: "How To Build a Self-Sovereign Identity Wallet?".

NOTE: Available at https://www.devteam.space/blog/how-to-build-a-self-sovereign-identity-wallet/.

DHL: "The Logistics Trend Radar. 5th Edition". DHE Trend Research.

NOTE: Available at https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-logistics-trend-radar-5thedition.pdf.

Di Salvo Mathew: "ACLU, EFF come out against blockchain for COVID-19 tracking". Decrypt.io. August 10, 2020.

NOTE: Available at https://decrypt.co/38218/aclu-eff-against-blockchain-covid-19-tracking-tracing.

DP-3T: "Protect infected users against Bluetooth® monitoring: ECDH key exchange #66". DP-3T project. Documents. Open issues. April 7, 2020.

NOTE: Available at https://github.com/DP-3T/documents/issues/66.

DRIVER+: "DRIVER+ project".

NOTE: Available at https://www.driver-project.eu.

EC: "Coronavirus Response". European Commission.

NOTE: Available at https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response_en.

Communication from the Commission COM(2020) 112 final of 13 March 2020 to the European Parliament, the European Council, the Council, the European Central Bank, the European Investment Bank and the Eurogroup. Coordinated economic response to the COVID-19 Outbreak. European Commission.

NOTE: Available at https://eur-lex.europa.eu/resource.html?uri=cellar:91687006-6524-11ea-b735-01aa75ed71a1.0001.02/DOC_1&format=PDF.

Annexes (1 to 3) to the Communication from the Commission COM(2020) 112 final of 13 March 2020 to the European Parliament, the European Council, the Council, the European Central Bank, the European Investment Bank and the Eurogroup. Coordinated economic response to the COVID-19 Outbreak. European Commission.

NOTE: Available at https://eur-lex.europa.eu/resource.html?uri=cellar:91687006-6524-11ea-b735-01aa75ed71a1.0001.02/DOC_2&format=PDF.

Communication from the Commission COM(2020) 143 final of 2 April 2020 to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Coronavirus response. Using every available euro in every way possible to protect lives and livelihoods. European Commission.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0143&from=EN.

Commission recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data". European Commission, Official Journal of the European Union, OJEU.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518&from=EN.

Communication from the Commission COM(2020) 2523 final of 16 April 2020: "Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection". European Commission.

NOTE: Available at https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf.

Communication from the Commission COM(2020) 456 final of 27 May 2020 to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: "Europe's moment: Repair and Prepare for the Next Generation". European Commission.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0456&from=EN.

Commission implementing decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic. European Commission. Official Journal of the European Union, OJEU. July 16, 2020.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:227I:FULL&from=EN.

"Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps". European Commission. Press release. June 16, 2020.

NOTE: Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043.

"EU Federation Gateway Service open issues". European Commission. GitHub.com.

NOTE: Available at https://github.com/eu-federation-gateway-service/efgs-federation-gateway/issues.

"EBSI: Experience the future with the European Blockchain Services Infrastructure". European Commission. Connecting Europe Facility, CEF, Digital.

NOTE: Available at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI.

"Rolling Plan for ICT Standardisation 2020. COVID-19 Addendum". European Commission.

NOTE: Available at https://ec.europa.eu/docsroom/documents/41867/attachments/1/translations/en/renditions/native.

ECDC: "Contact tracing: Public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union - second update". European Centre for Disease Control and Prevention. Technical report. Stockholm, April 9, 2020.

NOTE: Available at https://www.ecdc.europa.eu/en/covid-19-contact-tracing-public-health-management.

ECDC: "Contact tracing for COVID-19: current evidence, options for scale-up and an assessment of resources needed". European Centre for Disease Control and Prevention. Technical report. Stockholm, May 5, 2020.

NOTE: Available at https://www.ecdc.europa.eu/en/publications-data/contact-tracing-covid-19-evidence-scale-up-assessment-resources.

ECDC: "Mobile applications in support of contact tracing for COVID-19 - A guidance for EU EEA Member States". European Centre for Disease Control and Prevention. Stockholm, June 10, 2020.

NOTE: Available at https://www.ecdc.europa.eu/en/publications-data/covid-19-mobile-applications-support-contact-tracing.

ECDC: "Guidelines for the implementation of non-pharmaceutical interventions against COVID-19". European Centre for Disease Control and Prevention. Stockholm, September 24, 2020.

NOTE: Available at https://www.ecdc.europa.eu/en/publications-data/covid-19-guidelines-non-pharmaceutical-interventions.

The Economist: "South Korea keeps COVID-19 at bay without a total lockdown". March 30, 2020.

NOTE: Available at https://www.economist.com/asia/2020/03/30/south-korea-keeps-covid-19-at-bay-without-a-total-lockdown.

EDPB: "Statement on the processing of personal data in the context of the COVID-19 outbreak". European Data Protection Board, EDPB. March 19, 2020.

NOTE: Available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

EDPB: "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak". European Data Protection Board, EDPB. April 21, 2020.

NOTE: Available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en.

eHEALTH Network: "Key documents page". The eHealth Network. October 19, 2020.

NOTE: Available at https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

eHEALTH Network: "Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. Version 1.0". The eHealth Network. April 15, 2020.

NOTE: Available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

eHEALTH Network: "Annex IV: Inventory mobile solutions against COVID-19" (annex to the 'Common EU Toolbox for Member States'). The eHealth Network. April 15, 2020.

NOTE: Available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_annex_en.pdf.

eHEALTH Network: "Interoperability guidelines for approved contact tracing mobile applications in the EU". The eHealth Network. May 13, 2020.

NOTE: Available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

eHEALTH Network: "Guidelines to the EU Member States and the European Commission on interoperability specifications for cross-border transmission chains between approved apps (European Proximity Tracing. An Interoperability Architecture)". The eHealth Network. June 16, 2020.

NOTE: Available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilitydetailedelements_en.pdf.

ERS: "COVID-19: Guidelines and recommendations directory". European Respiratory Society.

NOTE: Available at https://www.ersnet.org/covid-19-guidelines-and-recommendations-directory.

ETSI: "ETSI releases white paper on the role of standards for ICT to mitigate the impact of a pandemic". Press release. Sophia Antipolis, May 28, 2020.

NOTE: Available at https://www.etsi.org/newsroom/press-releases/1772-2020-05-etsi-releases-white-paper-on-the-role-of-standards-for-ict-to-mitigate-the-impact-of-a-pandemic?jjj=1591293257419.

EUROPARL: "Joint motion for a resolution pursuant to Rule 132(2) and (4) of the Rules of Procedure replacing the following motions: B9-0143/2020 (Renew), B9-0144/2020 (PPE), B9-0146/2020 (S&D) and B9-0147/2020 (Verts/ALE) on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP))". European Parliament. April 15, 2020.

NOTE: Available at https://www.europarl.europa.eu/doceo/document/RC-9-2020-0143_EN.html.

EUROPARL: "European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP))". European Parliament. April 17, 2020.

NOTE: Available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.html.

Europa Press: "El Gobierno insta a la población a descargarse la app 'Radar COVID' para frenar la transmisión del virus". ElEconomista.es. September 8, 2020.

NOTE: Available at https://www.eleconomista.es/nacional/noticias/10758352/09/20/El-Gobierno-insta-a-la-poblacion-a-descargarse-la-app-Radar-Covid-para-frenar-la-transmision-del-virus.html.

EUvsVIRUS: "#EUvsVirus challenge. Matchathon and hackathon". EUvsVirus.org.

NOTE: Available at https://www.euvsvirus.org/.

Evernym: "Responding to the COVID-19 Challenge with Verifiable Credentials". Evernym, Inc.

NOTE: Available at https://www.evernym.com/covid19-creds/.

Fernández, Manuel: "Europa podría tener una app única para luchar contra el coronavirus". El Español/Omicrono. April 4, 2020.

NOTE: Available at https://www.elespanol.com/omicrono/software/20200404/europa-podria-tener-app-unica-luchar-coronavirus/479952504_0.html.

Fernández, Samuel: "Singapur ha creado la 'app' más avanzada para prevenir contagios por coronavirus y así podría ser adaptada en España". XatakaMóvil.com. April 3, 2020.

NOTE: Available at https://www.xatakamovil.com/aplicaciones/singapur-ha-creado-app-avanzada-para-prevenir-contagios-coronavirus-asi-podria-ser-adaptada-espana.

Ferretti, L. et alter: "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing". Science 368, eabb6936 (2020).

NOTE 1 Available at: https://dx.doi.org/10.1126/science.abb6936.

NOTE 2: Available at https://science.sciencemag.org/content/368/6491/eabb6936.

FIfF: "Data Protection Impact Assessment for the Corona App", Forum of Computer Professionals for Peace and Societal Responsibility, FIfF. April 29, 2020.

NOTE: Available at https://www.fiff.de/dsfa-corona-file-en/at_download/file.

García-Jaen, Braulio: "El reto de rastrear el virus sin perder derechos". ElPaís. June 26, 2020.

NOTE: Available at https://elpais.com/internacional/2020-06-25/el-reto-de-rastrear-el-virus-sin-perder-derechos.html.

Glick, Alexis: "A common-sense approach to coronavirus crisis". CNN.com. March 10, 2020.

NOTE: Available at https://edition.cnn.com/2020/03/09/opinions/coronavirus-businesses-common-sense-glick/index.html.

González-Martínez, Juan; Fernando Pérez-González; Luis Pérez-Freire & David Chaves-Diéguez: "Abriendo la caja de Pandemia: por qué necesitamos repensar el rastreo digital de contactos". CYPRIAN (Cybersecurity, Privacy and Anonimity joint Lab of Gradiant & the University of Vigo). May 1, 2020.

NOTE: Available at https://www.gradiant.org/wp-content/uploads/2020/05/Informe-Cyprian-contact-tracing_v1-1.pdf.

Goodes, Grant: "Most Government-Sponsored COVID-19 Contact Tracing Apps Are Insecure and Risk Exposing Users' Privacy and Data". Guardsquare. June 18, 2020.

NOTE: Available at https://www.guardsquare.com/en/blog/report-proliferation-covid-19-contact-tracing-apps-exposes-significant-security-risks.

DoH (Gov't of Ireland): "Department of Health and the HSE announce the publication of the Covid Tracker App Data Protection Impact Assessment and source code". Government of Ireland. Press release. June 29, 2020.

NOTE: Available at https://www.gov.ie/en/press-release/bb5d9-department-of-health-and-the-hse-today-announce-the-publication-of-the-covid-tracker-app-data-protection-impact-assessment-and-source-code/.

GOVTECH (Gov't of Singapore): "Tearing down the TraceTogether Token!" (video). Government Technology Agency of Singapore. July 5, 2020.

GOVTECH (Gov't of Singapore): "Improving TraceTogether through community engagement". Government Technology Agency of Singapore. July 6, 2020.

NOTE: Available at https://www.tech.gov.sg/media/technews/2020-07-06-tracetogether-token-teardown.

GSMA: "Digital Health. A health system strengthening tool for developing countries". GSM Association. June, 2020.

NOTE: Available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/06/Digital-Health-June-2020.pdf.

Hart Vi; Divya Siddarth; Bethan Cantrell; Lila Tretikov; Peter Eckersley; John Langford; Scott Leibrand; Sham Kakade; Steve Latta; Dana Lewis; Stefano Tessaro and Glen Weyl: "Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks". Harvard University. Edmond J. Safra Center for Ethics. COVID-19 Rapid Response Impact Initiative (R2I2) | White Paper 5. April 3, 2020.

NOTE: Available at https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf.

Harvard University: "COVID-19 response". Harvard University. Edmond J. Safra Center for Ethics. COVID-19 Rapid Response Impact Initiative (R2I2).

NOTE: Available at https://ethics.harvard.edu/covid-19-response.

Hayward Andrew: "Privacy Bug Found in Apple, Google COVID-Tracing Framework". Decrypt.co. September 3, 2020.

NOTE: Available at https://decrypt.co/40765/privacy-bug-found-apple-google-covid-tracing-framework.

HEALTH IT: "Interoperability Proving Ground" (a list of interoperability projects for COVID-19 pandemic). HealthIT.gov.

NOTE: Available at https://www.healthit.gov/techlab/ipg/?tag=COVID-19.

Hemestberger, Lea: "Call for Solutions: Outsmarting the Corona Pandemic with Digital Innovation". Open & Agile Smart Cities, OASC. April 14, 2020.

NOTE: Available at https://oascities.org/call-for-solutions-outsmarting-the-corona-pandemic-with-digital-innovation/.

IDB "Is data privacy the price we must pay to survive a pandemic?". Inter-American Development Bank Group. Discussion paper no. IDB-DP-00763. April, 2020.

NOTE: Available at https://publications.iadb.org/publications/english/document/Is_Data_Privacy_The_Price_We_Must_Pay_to_Survive_a_Pandemic.pdf.

IDB LAB. "COVID APP infographics": Inter-American Development Bank Group's innovation laboratory. August 18, 2020.

NOTE: Available at https://public.flourish.studio/story/394908/.

IEEE: "COVID-19. Your IEEE resources". IEEE. Spectrum.

NOTE: Available at https://spectrum.ieee.org/static/covid19-ieee-resources.

IEEE SA: "Statement Regarding the Ethical Implementation of Artificial Intelligence Systems (AIS) for Addressing the COVID-19 Pandemic". IEEE Standards Association.

NOTE: Available at https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/gieais-covid.pdf.

INNOVADORES: "¿Quién vigila a las apps que vigilan la Covid-19? El MIT". Innovadores by Inndux. July 10, 2020.

NOTE: Available at https://innovadores.inndux.com/es/mit-desarrolla-sistema-vigilar-apps-rastreos-covid-19/.

ISO/IEC 27002:2013: "Information technology -- Security techniques -- Code of practice for information security controls". International Organization for Standardization. October, 2013.

NOTE: Available at https://www.iso.org/standard/54533.html.

ISO: "COVID-19: National resources". International Organization for Standardization. September 1, 2020.

NOTE: Available at https://www.iso.org/covid19-members.

ITU: "Global network resiliency platform". International Telecommunications Union.

NOTE: Available at https://reg4covid.itu.int/.

ITU: "First overview of key initiatives in response to COVID-19". International Telecommunications Union. May, 2020.

NOTE: Available at https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/REG4COVID/2020/Summary_Key_Covid19_Initiatives.pdf.

ITU: "Roadmap to ITU-T e-Health Standardization". International Telecommunications Union.

NOTE: Available at https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/rm/ehealth.aspx.

ITU: "AI for Good: Global Impact". International Telecommunications Union ITUNews magazine, no. 2. 2020.

NOTE: Available at https://www.itu.int/en/itunews/Documents/2020/2020-02/2020_ITUNews02-en.pdf.

Jaimes Nicolas: "TousAntiCovid: combien de téléchargements du nouveau StopCovid?". JournalduNet.com (JDN). October 27, 2020.

NOTE: Available at https://www.journaldunet.com/media/publishers/1490935-tousanticovid-combien-de-telechargements-du-nouveau-stopcovid/.

Johnson Khari: "What privacy-preserving coronavirus tracing apps need to succeed". VentureBeat. April 23, 2020.

NOTE: Available at https://venturebeat.com/2020/04/13/what-privacy-preserving-coronavirus-tracing-apps-need-to-succeed/.

Kelion Leo: "Coronavirus: First Google/Apple-based contact-tracing app launched". BCC News. May 26, 2020.

NOTE: Available at https://www.bbc.com/news/technology-52807635.

Kerravala Zeus: "3 factors for implementing contact tracing in the workplace". CIO.com. July 24, 2020.

NOTE: Available at https://www.cio.com/article/3567199/3-factors-for-implementing-contact-tracing-in-the-workplace.html.

Ketels Christian and J. Peter Clinch: "Acting now while preparing for tomorrow: Competitiveness upgrading under the shadow of COVID-19". Harvard Business School. Institute for Strategy and Competitiveness, ISC. ISC Working Paper. April 29, 2020.

NOTE: Available at https://www.isc.hbs.edu/Documents/pdf/Preparing%20for%20Tomorrow_Country%20Level_ISC%20WP%20version_04-29-20.pdf.

Koralnik Igor J. and Kenneth L. Tyler: "COVID-19: A Global Threat to the Nervous System". American Neurological Association. Annals of Neurology. June 1, 2020.

NOTE: Available at https://dx.doi.org/10.1002/ana.25807.

Kyodo: "Japan's coronavirus contact-tracing app launched amid privacy concerns". The Japan Times. June 19, 2020.

NOTE: Available at https://www.japantimes.co.jp/news/2020/06/19/national/japan-contact-tracing-app-launched/.

Kuribayashi, Fumiko: "コロナ追跡アプリ、政府主導で　グーグルとアップル要求". Asahi.com. May 12, 2020.

NOTE: Available at https://www.asahi.com/articles/ASN5D5VLHN58ULFA01Y.html.

Ledger Insights: "IBM, R3, Mastercard join open source digital identity consortium". LedgerInsights.com. April, 2020.

NOTE: Available at https://www.ledgerinsights.com/trust-over-ip-digital-identity-consortium-ibm-r3-mastercard/.

LFPH: "TCN Coalition and LFPH have merged". Linux Foundation Public Health, LFPH.

NOTE: Available at https://www.lfph.io/tcn-coalition/.

Lomas Natasha: "How will Europe's coronavirus contact-tracing apps work across borders?". TechCrunch.com. May 15, 2020.

NOTE: Available at https://techcrunch.com/2020/05/15/how-will-europes-coronavirus-contacts-tracing-apps-work-across-borders/.

Lorenzo Antonio: "La app Radar COVID se 'pelea' con los móviles viejos y con los más nuevos de Huawei®". ElEconomista.es/Tecnología. September 20, 2020.

NOTE: Available at https://www.eleconomista.es/tecnologia/noticias/10778049/09/20/La-app-Radar-Covid-se-pelea-con-los-moviles-viejos-y-con-los-mas-nuevos-de-Huawei.html.

Martínez Martínez Ricard: "Protección de datos y geolocalización en la Orden SND/297/2020". Expansión/Hay Derecho. March 31, 2020.

NOTE: Available at https://hayderecho.expansion.com/2020/03/31/proteccion-de-datos-y-localizacion-en-la-orden-snd-297-2020/.

Marzo Portera Ana: "La inoportuna doctrina de las autoridades europeas de protección de datos frente al Covid-19". Expansión/Hay Derecho. March 18, 2020.

NOTE: Available at https://hayderecho.expansion.com/2020/03/18/la-inoportuna-doctrina-de-las-autoridades-europeas-de-proteccion-de-datos-frente-al-covid-19/.

Méndez Manuel Ángel: "Bronca de Protección de Datos al Gobierno por falta de transparencia con la 'app' COVID". ElConfidencial. June 23, 2020.

NOTE: Available at https://www.elconfidencial.com/tecnologia/2020-06-23/aepd-sedia-carme-artigas-nadia-calvino-app-rastreo-contactos-covid_2652551/.

Merchán Montaña and Félix Serrano: "DiGital ReVolution".

NOTE: Available at https://digitalrevolution.info/.

Merkur: "Corona-App: Start-Termin jetzt fix? Infos aus 'Regierungskreisen' durchgesickert". Merkur.de. June 12, 2020.

NOTE: Available at https://www.merkur.de/politik/coronavirus-app-regierung-deutschland-google-apple-tracing-gesetz-uebertragung-datenschutz-zr-13716804.html.

mHEALTH HUB: "COVID-19 apps hub repository". European Innovation and Knowledge mHealth Hub. Andalusian Agency for Healthcare Quality.

NOTE 1: Available at https://doi.org/10.1038/d41586-020-01578-0.

NOTE 2: Available at https://mhealth-hub.org/mhealth-solutions-against-covid-19.

Morley Jessica, Josh Cowls, Mariarosaria Taddeo & Luciano Floridi: "Ethical guidelines for COVID-19 tracing apps". Nature 582, 29-31 (2020).

NOTE: Available at https://www.nature.com/articles/d41586-020-01578-0.

Nadal M. Victoria S. "La privacidad de las apps de contagio: prioridad en Europa, cuestión secundaria en Asia". El País/Tecnología. August 30, 2020.

NOTE: Available at https://elpais-com.cdn.ampproject.org/c/s/elpais.com/tecnologia/2020-08-29/la-privacidad-de-las-apps-de-contagio-prioridad-en-europa-cuestion-secundaria-en-asia.html?outputType=amp.

Nature: "Show evidence that apps for COVID-19 contact-tracing are secure and effective". Nature 580, 563 (2020).

NOTE 1: Available at https://doi.org/10.1038/d41586-020-01264-1.

NOTE 2: Available at https://www.nature.com/articles/d41586-020-01264-1.

NATURE: "COVID research updates". October 28, 2020.

NOTE: Available at https://www.nature.com/articles/d41586-020-00502-w.

NEWTON Casey: "Why Bluetooth® apps are bad at discovering new cases of COVID-19". TheVerge.com. April 10, 2020.

NOTE: Available at https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth®-coronavirus-flaws-public-health.

NSAI: "COVID-19 Resources". National Standards Authority of Ireland, NSAI.

NOTE: Available at https://www.nsai.ie/covid-19/.

O'Dowd Kris, Keerthi M. Nair, Parnia Forouzandeh, Snehamol Mathew, Jamie Grant, Ruth Moran, John Bartlett, Jerry Bird and Suresh C. Pillai: "Face Masks and Respirators in the Fight Against the COVID-19 Pandemic: A Review of Current Materials, Advances and Future Perspectives". July 29, 2020.

NOTE: Available at https://www.mdpi.com/1996-1944/13/15/3363/pdf.

O'Neill Patrick Howell: "Bluetooth® contact tracing needs bigger, better data". MIT Technology Review. April 22, 2020.

NOTE: Available at https://www.technologyreview.com/2020/04/22/1000353/bluetooth®-contact-tracing-needs-bigger-better-data/.

O'Neill Patrick Howell, Tate Ryan-Mosley and Bobbie Johnson: "COVID Tracing Tracker. A flood of coronavirus apps are tracking us. Now it's time to keep track of them". MIT Technology Review. May 7, 2020.

NOTE: Available at https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

OECD: "Beyond Containment: Health systems responses to COVID-19 in the OECD". Organization for Economic Cooperation and Development, OECD. Paris, April 16, 2020.

NOTE: Available at https://read.oecd-ilibrary.org/view/?ref=119_119689-ud5comtf84&title=Beyond_Containment:Health_systems_responses_to_COVID-19_in_the_OECD.

OECD: "Cities Policy Responses". Organization for Economic Cooperation and Development, OECD. Paris, July 23, 2020.

NOTE: Available at https://read.oecd-ilibrary.org/view/?ref=126_126769-yen45847kf&title=Coronavirus-COVID-19-Cities-Policy-Responses.

Oliver Nuria:. "Rastreando el virus: 'apps', personas y más". El Indempendiente. August 22, 2020.

NOTE: Available at https://www.elindependiente.com/opinion/2020/08/22/rastreando-el-virus-apps-personas-y-mas/amp/?s=08.

Ollero Daniel J.: "Protección de Datos investiga la app del Gobierno para rastrear 'infectados de Covid-19'". El Mundo. May 21, 2020.

NOTE: Available at https://amp.elmundo.es/tecnologia/2020/05/21/5ec695edfc6c83610d8b4594.html.

PACT: "ImPACT 2020. Technology and Public Health Perspectives on Private Automated Contact Tracing". PACT project.

NOTE: Available at https://pact.mit.edu/impact-2020/.

Párraga Navarro Antonio et alter: "Open Coronavirus project repository". GitHub.com.

NOTE: Available at https://github.com/open-coronavirus.

PEPP-PT: "Data protection and information security architecture. Ilustrated on German implementation". Pan-European Privacy-Preserving Proximity Tracing. Documentation. GitHub.com. April 20, 2020.

NOTE: Available at https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany.pdf.

Pérez Enrique: "España se une al proyecto europeo PEPP-PT y abre la puerta a utilizar la geolocalización de los móviles para rastrear el COVID-19". Xataka.com. April 20, 2020.

NOTE: Available at https://www.xataka.com/aplicaciones/espana-se-une-al-proyecto-europeo-pepppt-abre-puerta-a-utilizar-geolocalizacion-moviles-para-rastrear-covid-19.

Pérez-colomé Jordi: "La ingeniera española que lidera la 'app' europea de rastreo de contagios: 'No será un estado de vigilancia'". El País/Tecnología. April 16, 2020.

NOTE: Available at https://elpais.com/tecnologia/2020-04-15/la-ingeniera-espanola-que-lidera-la-app-europea-de-rastreo-de-contagios-no-debe-ser-un-estado-de-vigilancia.html.

PI: "Apps and COVID-19". PrivacyInternational.org.

NOTE: Available at https://privacyinternational.org/examples/apps-and-covid-19.

Posch Maya: "Teardown of the Singaporean COVID-19 TraceTogether token". Hackaday.com. June 25, 2020.

NOTE: Available at https://hackaday.com/2020/06/25/teardown-of-the-singaporean-covid-19-tracetogether-token/.

Powers Benjamin: "Decentralized Protocol Removed From EU Contact Tracing Website Without Notice". CoinDesk.com. April 17, 2020.

NOTE: Available at https://www.coindesk.com/decentralized-protocol-removed-from-eu-contact-tracing-website-with-no-notice.

Preukschat Alex: "The State of Digital Identity Wallets – Darrell O'Donnell – Webinar 22". SSIMeetup. February 21, 2019.

NOTE: Available at https://ssimeetup.org/state-digital-identity-crypto-wallets-darrell-odonnell-webinar-22/.

Quevedo Álex: "RASTRAR app". GitHub.com.

NOTE: Available at https://github.com/alexmonkeype/rastrar-app.

RFI: "France rolls out new COVID tracking app 'TousAntiCovid'". RFI. October 22, 2020.

NOTE: Available at https://www.rfi.fr/en/france/20201022-france-rolls-out-new-covid-19-mobile-tracking-app-tous-anti-covid-stopcovid.

Roxanne: "Only 17% of Singapore population downloaded TraceTogether app, experts urge to make it mandatory". The Online Citizen. May 5, 2020.

NOTE: Available at https://www.onlinecitizenasia.com/2020/05/05/only-17-of-singapore-population-downloaded-tracetogether-app-experts-urge-to-make-it-mandatory/.

Rubio-Romero Juan Carlos, María del Carmen Pardo-Ferreira, Juan Antonio Torrecilla-García and Santiago Calero-Castro: "Disposable masks: Disinfection and sterilization for reuse, and non-certified manufacturing, in the face of shortages during the COVID-19 pandemic". Safety Science, Volume 129. May 13, 2020.

NOTE 1: Available at https://doi.org/10.1016/j.ssci.2020.104830.

NOTE 2: Available at https://doi.org/10.1016/j.ssci.2020.104830.

Sato Yukiko: "AppleとGoogleのAPI採用新型コロナ通知アプリ開発は今、どの段階にあるのか". ITmedia.co.jp. May 24, 2020.

NOTE: Available at https://www.itmedia.co.jp/news/articles/2005/24/news012.html.

Sepkowitz Kent: "Eye-opening South Korea study on Covid-19". CNN.com. May 1, 2020.

NOTE: Available at https://edition.cnn.com/2020/04/30/opinions/eye-opening-south-korea-study-on-covid-19-sepkowitz/index.html.

Shankari et alter: "COVID-19 tracing projects". GitHub.com.

NOTE: Available at https://github.com/shankari/covid-19-tracing-projects.

Sharwood Simon: "Europe publishes draft rules for coronavirus contact-tracing app development, on a relaxed schedule". TheRegister.com. April 17, 2020.

NOTE: Available at https://www.theregister.com/2020/04/17/european_contact_tracing_app_spec/.

Stanley Jay & Jennifer Stisa Granick: "The Limits of Location Tracking in an Epidemic". American Civil Liberties Union (ACLU). April 8, 2020.

NOTE: Available at https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic.

TECH TEAM (Gov't of Japan): "接触確認アプリ及び関連システム仕様書（案） ［概要". Japan's Information and Communication Technology (IT) General Strategy Office. Government CIO Portal. May 17, 2020.

NOTE: Available at https://cio.go.jp/sites/default/files/uploads/documents/techteam_20200517_01.pdf.

TECH TEAM (Gov't of Japan): "接触確認アプリ及び関連システム仕様書（案）」に対するプライバシー及びセキュリティ上の評価及びシステム運用上の留意事項（案）の概要". Japan's Information and Communication Technology (IT) General Strategy Office. Government CIO Portal. May 17, 2020.

NOTE: Available at https://cio.go.jp/sites/default/files/uploads/documents/techteam_20200517_03.pdf.

Temple, James: "Why contact tracing may be a mess in America". MIT Technology Review. May 16, 2020.

NOTE: Available at https://www.technologyreview.com/2020/05/16/1001787/why-contact-tracing-may-be-a-mess-in-america/.

Troncoso Carmela et alter: "Decentralized Privacy-Preserving Proximity Tracing. Overview of Data Protection and Security". GitHubUserContent.com. April 3, 2020.

NOTE: Available at https://raw.githubusercontent.com/DP-3T/documents/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf.

Turner Roland: "TraceTogether Token Teardown Time!". RolandTurner.com. June 22, 2020.

NOTE: Available at https://rolandturner.com/2020/06/22/TraceTogether_Token_Teardown_Time.

UNESCO: "Statement on COVID-19: ethical considerations from a global perspective". United Nations Educational, Scientific and Cultural Organization. UNESDOC. SHS/IBC-COMEST/COVID-19 REV. Paris, April 6, 2020.

NOTE: Available at https://unesdoc.unesco.org/ark:/48223/pf0000373115.

uPORT: "uPort website".

NOTE: Available at https://www.uport.me/.

Vila Pueyo Xavier: "Self-Sovereign Identity in the age of a global pandemic: Validated ID joins the Covid Credentials Initiative". Validated ID. Blog.

NOTE: Available at https://www.validatedid.com/post-de/self-sovereign-identity-in-the-age-of-a-global-pandemic-validated-id-joins-the-covid-credentials-initiative.

Vandamme Anne-Mieke & ToTran Nguyen: "Belgium - concerns about coronavirus contact-tracing apps". Nature 581, 384 (2020).

NOTE 1: Available at https://doi.org/10.1038/d41586-020-01552-w.

NOTE 2: Available at https://www.nature.com/articles/d41586-020-01552-w.

Veale Michael: "Security and privacy analysis of the document 'ROBERT: ROBust and privacy-presERving proximity Tracing'". The DP-3T Project. April 22, 2020.

NOTE: Available at https://github.com/DP-3T/documents/blob/master/Security%20analysis/ROBERT%20-%20Security%20and%20privacy%20analysis.pdf.

Ventura Víctor: "Ocho países europeos estudian una app que detecte los contactos cercanos entre personas para contener el virus". ElEconomista.es. April 2, 2020.

NOTE: Available at https://www.eleconomista.es/internacional/noticias/10459062/04/20/Ocho-paises-europeos-estudian-una-app-que-detecte-los-contactos-cercanos-entre-personas-para-contener-el-virus.html.

Von Arx Sydney, Isaiah Becker-Mayer, Daniel Blank, Jesse Colligan, Rhys Fenwick, Mike Hittle; Mark Ingle, Oliver Nash, Victoria Nguyen, James Petrie, Jeff Schwaber, Zsombor Szabo, Akhil Veeraghanta; Mikhail Voloshin, Tina White & Helen Xue: "Slowing the Spread of Infectious Diseases Using Crowdsourced Data". COVIDWatch.org. March 20, 2020.

NOTE: Available at https://f.hubspotusercontent30.net/hubfs/7663287/covid_watch_whitepaper.pdf?__hssc=109102170.2.1599420704777&__hstc=109102170.b7d80f97441e29781e66b84d6c567fda.1599159739483.1599180806730.1599420704777.3&__hsfp=2020963374&hsCtaTracking=d5f7031a-eb86-4e35-af5f-91708a4e7b9b%7Cd71fe660-8b64-4fef-99c8-1eb56a63976a.

W3C: "Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web". World Wide Web Consortium, W3C. November 19, 2019.

NOTE: Available at https://www.w3.org/TR/vc-data-model/.

WHO: "Critical preparedness, readiness and response actions for COVID-19". World Health Organization, WHO. Interim guidance. March 22, 2020.

NOTE: Available at https://apps.who.int/iris/rest/bitstreams/1272587/retrieve.

WHO: "Considerations in the investigation of cases and clusters of COVID-19". World Health Organization, WHO. Interim guidance. April 2, 2020.

NOTE: Available at https://apps.who.int/iris/rest/bitstreams/1274007/retrieve.

WHO: "Contact tracing in the context of COVID-19". World Health Organization, WHO. May 10, 2020.

NOTE: Available at https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19.

WIKIPEDIA: "Contact tracing".

NOTE: Available at https://en.wikipedia.org/wiki/Contact_tracing.

WIKIPEDIA: "Digital contact tracing".

NOTE: Available at https://en.wikipedia.org/wiki/Digital_contact_tracing.

WIKIPEDIA: "BlueTrace".

NOTE: Available at https://en.wikipedia.org/wiki/BlueTrace.

WIKIPEDIA: "TraceTogether".

NOTE: Available at https://en.wikipedia.org/wiki/TraceTogether.

WIKIPEDIA: "TCN protocol".

NOTE: Available at https://en.wikipedia.org/wiki/TCN_Protocol.

WMO: "Climatological, Meteorological and Environmental Factors in COVID-19 Pandemic". World Meteorological Organization, WMO. Porter sessions. August 3-6, 2020.

NOTE: Available at https://covid19covenv-agu.ipostersessions.com/?s=covid19_covenv_gallery.

Zissman Marc: "PACT: Private Automated Contact Tracing" (presentation). IEEE EMBS 2020 Annual Conference. July 24, 2020.

NOTE: Available at https://pact.mit.edu/wp-content/uploads/2020/07/Zissman-PACT-Talk-for-IEEE-EMBS-2020.pdf.

Annex B:
Change History

Date	Version	Information about changes
November 2020	0.1.8	(ETSI) review of draft with revison mark (13/11/2020)
November/December 2020	0.1.9	Rapporteur's review of draft with revison mark (17/11/2020)

History

Document history		
V1.1.1	February 2021	Publication