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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

Copyright Notification

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/