ETSI GS E4P 003 V1.1.1 (2021-04)

Europe for Privacy-Preserving Pandemic Protection (E4P); High level requirements for pandemic contact tracing systems using mobile devices

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
DGS/E4P-003

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 pandemic 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 as a complementary solution 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 deployed in many different countries. In particular, mobile devices with their contact tracing applications can support public health authorities in controlling and containing the pandemic. E4P has been created to provide a technical answer to pandemic crisis not limited to COVID-19 by specifying interoperable contact tracing systems.

1 Scope

The present document specifies the high level requirements for digital contact tracing systems operating by proximity detection, using mobile devices, which are practical to deploy and being compliant with the applicable laws and regulations, as well as providing a seamless continuity of pandemic contact tracing for people travelling between countries.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

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 necessary for the application of the present document.

[1] ETSI EN 301 549 (V3.1.1): "Accessibility requirements for ICT products and services".

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] CEN/ISO 82304-2: "Quality Requirements Conformity Assessment".

[i.2] ETSI GS E4P 006 (V1.1.1): "Europe for Privacy-Preserving Pandemic Protection (E4P); Device-Based Mechanisms for pandemic contact tracing systems".

[i.3] ETSI GS E4P 008 (V1.1.1): "Europe for Privacy-Preserving Pandemic Protection (E4P); Back-End mechanisms for pandemic contact tracing systems".

[i.4] ETSI GS E4P 007: "Europe for Privacy-Preserving Pandemic Protection (E4P); Pandemic proximity tracing systems: Interoperability framework".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

CSIRT	Computer Security Incident Response Team
DCTS	Digital Contact Tracing System
ECDC	European Centre for Disease prevention and Control
EU	European Union
GDPR	General Data Protection Regulation
PII	Personally Identifiable Information
QR	Quick Response (code)
RFID	Radio Frequency IDentification
UX	User experience
WHO	World Health Organization

4 General description

4.1 Introduction

A Digital Contact Tracing System (DCTS) is a system that in the context of an epidemic, aims to warn its users that they have been in contact with users that have been diagnosed with the disease.

To facilitate the development and deployment of contact tracing systems that are efficient i.e. having a real impact in fighting a pandemic, interoperable and trusted by their users they need to be built on well-defined functional and legal requirements. This is the aim of the present document to provide a set of such well-founded high-level requirements.

The requirements in the present document take privacy concerns strongly into consideration. Note that the relevant requirements need to be completed with the applicable legislation of the country where the DCTS system is deployed (legislation such as the GDPR in the EU). The present document covers DCTS using proximity detection with mobile phones. These are the majority of DCTS that are in use or in development at the time of the writing of the present document. Some systems feature components such as token devices (electronic devices with limited capacity for communication and/or computation). Proposals have also been made of systems using elements communicating information from fixed locations (for example entrance of rooms, shops, buildings or other facilities) or linked to objects (for example via RFID tags). Depending on their adoptions, such more complex systems may be taken into account in a future version of the present document.

4.2 Objectives

The present document provides high level requirements for DCTS. The requirements are directed to entities that commission, design, implement, maintain in operational conditions, operate, monitor and supervise a digital contact tracing system.

4.3 A Digital Contact Tracing System

This clause describes a high level reference architecture of a DCTS using proximity detection which is further defined in the respective entities of the reference architecture in ETSI GS E4P 006 [i.2] and ETSI GS E4P 008 [i.3].

In the sequel, diagnosed means diagnosed with the disease that is the subject of the epidemic.

The main purpose of a DCTS is to warn its users when they were in contact with users that have been diagnosed.

In a high level description of a DCTS the essential elements are described as below.

User (U): The "User (U)" in the E4P reference architecture, interacting with the "Device (D)" via the interface represented by the reference point DU). The User is at risk when the DCTS determines the User was in relevant proximity with a diagnosed user.

Mobile Device: "Device (D)" is responsible for providing the proximity information (stored as proximity data), obtained from the Proximity Detection Method, by communicating with other Mobile Devices and communicating with the Infrastructure; via the Mobile Application. The Mobile Device supports the User interaction with the DCTS.

Mobile Application: software running on the Mobile Device, responsible for registering and managing proximity information, communicating with the Infrastructure, alerting the User that it was in close proximity with a diagnosed user (through a process called risk calculation) and notifying the Infrastructure that the User was diagnosed (a functional module inside the Mobile Device, that is not represented in the reference architecture but is refined in ETSI GS E4P 006 [i.2]).

Note that Mobile Application includes the software dedicated to these tasks irrespective of whether it is part of an application downloaded by the User or not (for example as included in the operating system of the Mobile Device).

Infrastructure: provides authoritative and trusted information to the Mobile Device. The main role of the Infrastructure is information sharing between Users via the Mobile Devices and Mobile Applications. Each Mobile Application is linked to an Infrastructure.

Federation: provides the means to interconnect (exchange information between) different Infrastructures, through a Federation Protocol (represented as the reference point BF), to provide interoperability of the different DCTS, in the sense of the full continuity of the proximity information and risk calculation and notification.

Proximity Detection Method: the method used by Mobile Devices for detecting proximity with diagnosed users (represented as the reference point DD). The proximity Detection Method use ephemeral identifiers that are broadcast by the Mobile Devices.

Contact Tracing Protocol: the protocol between Mobile Devices and the Infrastructure, used by the Mobile Application (represented by the reference point DB).

Federation Protocol: a protocol used to exchange information between different Infrastructures (represented by the reference point BF).

Health Authority: the authority overseeing the DCTS and endorsing the Mobile Application, the Infrastructure and the risk calculation method. The Health Authority is responsible for certifying the diagnosis of a User. The diagnosis is provided via a proxy e.g. a physician or a medical laboratory and typically entered in the Mobile Application by the User via e.g. scanning a QR code (represented as External Systems, out of the scope of the present document, with reference point BE).

Usually a country operates one DCTS but nothing prevents a DCTS to be used in several countries or a country using more than one DCTS.

Current DCTS are classified as centralized or decentralized.

Centralized systems are systems where the Mobile Application uploads identifiers of the relevant contacts of the User (as obtained by the Proximity Detection Method and risk calculation) to the Infrastructure when the User is diagnosed.

Decentralized systems are systems where the Mobile Application uploads the identifiers it used (its own identifiers, generated as part of the Proximity Detection Method) to the Infrastructure when the User is diagnosed.

In the centralized approach, the identifiers broadcast by a Mobile Device to identify itself are centrally generated (by the Infrastructure) whereas in a decentralized approach the identifiers are generated on the Mobile Device by the Mobile Application.

The risk calculation is done on the Mobile Device in the decentralized approach and in the Infrastructure in the centralized approach.

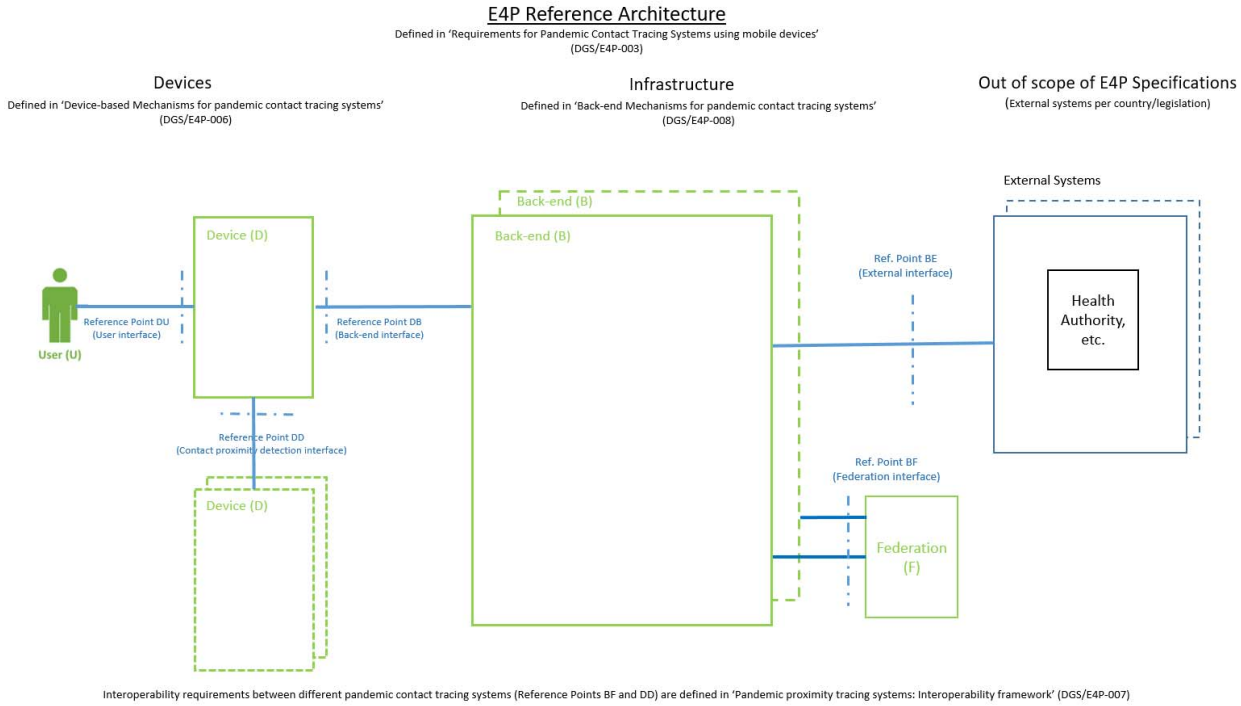

Figure 1: E4P High-level Reference Architecture

5 High level requirements

5.1 General

Sharing of epidemiological information:

[HL-GE-01] The DCTS may allow, based on consent and/or national law, to transmit anonymized, aggregated or pseudonymised data to national epidemiological and/or research institutions for analysis as well as transmission of aggregated data to national authorities and international agencies (e.g. WHO or ECDC).

Proliferation of applications:

[HL-GE-02] A DCTS should use only one Mobile Application per technological platform.

NOTE: By technological platform is meant a combination of hardware and operating system.

[HL-GE-03] The Health Authority shall inform the User of which Mobile Application to use.

[HL-GE-04] The Health Authority should monitor the digital platforms distributing applications for Mobile Devices and take the necessary actions whenever applications that may mislead the User are listed.

Monitoring effectiveness:

[HL-GE-05] The Health Authority should periodically monitor the effectiveness of the DCTS and of its interoperability with other DCTS via Federations.

[HL-GE-06] The DCTS (in particular the Infrastructure) should provide the functionalities for the monitoring of its effectiveness.

Epidemiological and medical updating:

[HL-GE-07] The Health Authority shall have the Mobile Application and the Infrastructure updated as soon as possible and no later than 15 days when relevant new epidemiological and medical information is known regarding the epidemic.

Availability of technology:

[HL-GE-08] The contact tracing capabilities should be supported by enough Mobile Devices with Bluetooth Low Energy connectivity to ensure the effectiveness of the DCTS.

[HL-GE-09] The contact tracing capability of the Mobile Device should be supported by enough operating systems to ensure the effectiveness of the DCTS.

5.2 Usability - User experience

Accessibility:

[HL-UX-01] Mobile Application shall meet the accessibility requirements set out in the relevant standards (such as the ETSI EN 301 549 [1]).

Performance and battery usage:

[HL-UX-02] The energy consumption of the Mobile Application shall be measured and quoted.

Information:

[HL-UX-03] User shall be informed about the working and the usage of the DCTS e.g. via the Mobile Application or on a web site.

5.3 Mobile Device

Proximity technology:

[HL-MD-01] Mobile Device shall possess the hardware capabilities to estimate the distance to another Mobile Device using the Proximity Detection Method with sufficient accuracy. When relevant, calibration methods shall be used.

5.4 Mobile Application

Proximity detection:

[HL-MA-01] Proximity detection method performance shall not be limited by Mobile Application runtime configuration e.g. running in a background mode or locked user interface.

[HL-MA-02] The Mobile Application shall be able to estimate and record the criteria set by the Health Authority, the proximity between Mobile Devices via Bluetooth Low Energy or other techniques.

[HL-MA-03] The Mobile Application shall advertise continuously its presence using an ephemeral identifier that permits to establish contact with other Mobile Applications in proximity.

[HL-MA-04] The Mobile Application should be able to advertise other Mobile Applications the country or the division within a country in which it is registered or the Health Authority overseeing it.

Physical proximity relevance:

[HL-MA-05] The Mobile Application should store ephemeral identifiers in proximity data when they are epidemiologically relevant according to the criterion sanctioned by the Health Authority (typically based on distance, time duration within a minimum distance).

Ephemeral identifiers:

[HL-MA-06] The ephemeral identifier sent by the Mobile Device shall be generated pseudo-randomly and change periodically to enhance the protection against eavesdropping, hacking and tracking by third parties.

[HL-MA-07] The ephemeral identifier shall include the information to identify the Mobile Device to send it push notifications, when needed by the Contact Tracing Protocol.

[HL-MA-08] It shall not be practical to persistently identify a mobile device from its ephemeral identifier.

Access to the source code:

[HL-MA-09] The technical specifications of the Contact Tracing Protocol shall be made available publicly.

[HL-MA-10] The part of the source code for the Mobile Application that is relevant to ensure the trust of the public shall be made available publicly as well as the relevant part of the source code of any specific libraries or software components.

[HL-MA-11] The part of the source code for the Mobile Application that is relevant to ensure the trust of the public should be made available publicly under the terms of an Open Source licence.

[HL-MA-12] The relevant part of the source code of any specific libraries or software components that is relevant to ensure the trust of the public should be made available publicly under the terms of an Open Source licence.

Epidemiologically relevant retention period for proximity data:

[HL-MA-13] The Mobile Application shall erase all proximity data older than the retention period defined by the Health Authority.

Information to users at risk:

[HL-MA-14] The Health Authority shall determine how to inform users identified as at risk by the DCTS, e.g. via the Mobile Application or by other means.

[HL-MA-15] Safeguards shall be put in place to secure data collection, storage and sharing policies of the information related to users at risk.

Timing of notification of users at risk:

[HL-MA-16] Users identified as at risk shall be notified through their Mobile Device in a delay of at most 12 hours.

Information to be provided to the user:

[HL-MA-17] Users at risk shall be informed about potential infection due to a close contact with a diagnosed person and what to do next.

[HL-MA-18] The content of the message sent to a User at risk shall be determined by the Health Authority.

[HL-MA-19] The Health Authority, depending on the national laws, may contact directly the User that was in contact with a diagnosed user.

[HL-MA-20] The User shall be informed, at the moment of the Mobile Application installation or first usage, that he/she can be contacted by the Health Authority in case the user is determined at risk.

[HL-MA-21] The User shall be informed, at the moment of the Mobile Application installation or its first usage, of the categories of data which will be collected by the Mobile Application and transmitted to the Infrastructure and how and why their data may be processed and used.

User authentication:

[HL-MA-22] The Mobile Application shall make use of the user authentication methods available on the Mobile Device to limit access to information.

Use of libraries and third party code:

[HL-MA-23] When third party libraries are used, they shall be kept up to date.

[HL-MA-24] Vetting of libraries and third party code shall be exercised to insure they can be integrated securely in the Mobile Application.

Handling insecure Mobile Devices:

[HL-MA-25] The Mobile Application shall consider that not all Mobile Devices run the latest versions of operating systems, some may be running vulnerable or modified software, and some built-in security functions may not be available.

UX standards:

[HL-MA-26] Considerations should be given to the relevant works (such as CEN/ISO 82304-2 [i.1]) that could help assessing medical safety, usability, safety of personal data and technical quality of health apps and issue a Health App Quality Label.

Mobile Application update notification:

[HL-MA-27] The Mobile Application shall regularly check for the availability of updates (not less than once a day) and notify the User of this availability and how to install the update.

5.5 Infrastructure

Code produced to confirm cases:

[HL-IN-01] The data created by the Health Authority to confirm a case shall be generated pseudo-randomly and be single-use.

NOTE: This ensures that it cannot be used by malicious individuals to pollute the data collected by the Infrastructure.

[HL-IN-02] This data shall be presented in a user-friendly format (e.g. as a QR code) to avoid input error from the User.

Scalability of Infrastructure:

[HL-IN-03] The DCTS shall be capable of supporting the estimated number of Mobile Devices in the geographical area it covers as well as the additional load generated by its interconnections with other Infrastructures.

Infection confirmation:

[HL-IN-04] Only the Health Authority or other authorized parties such as medical test laboratories shall be entitled to confirm a user was diagnosed.

[HL-IN-05] Only the Health Authority or other authorized parties such as medical test laboratories may provide the User the necessary data (see **HL-IN-01** and **HL-IN-02)** so that the User can declare it was diagnosed to the DCTS or alternatively the Health Authority or other authorized parties may declare the user was diagnosed to the DCTS after the consent of the User.

5.6 Security

Secure software development:

[HL-SE-01] Good practices shall be followed with regard to secure coding principles, secure design principles for the development of the Mobile Application, the Infrastructure and the Federation.

[HL-SE-02] The latest and up to date development environments should be used for the development of the Mobile Application, the Infrastructure and the Federation.

[HL-SE-03] Adequate tests shall be performed on the software for the Mobile Application, the Infrastructure and the Federation, using automated tools for testing and integration, which cover not only functional aspects, but also security, code quality, (static and dynamic) code analysis tools.

[HL-SE-04] Threats to the Infrastructure and any related services shall be assessed and minimized.

[HL-SE-05] Threats to the Federation and any related services shall be assessed and minimized.

[HL-SE-06] Threats to the environments used for the development of Mobile Application, the Infrastructure and the Federation shall be assessed and minimized.

NOTE: Cyber attackers often target software developers, system administrators, development platforms, because they may have system passwords, sensitive credentials, access to source code, access rights to sensitive assets, passwords, etc.

Built-in security for Mobile Application:

[HL-SE-07] The Mobile Application shall make best use of the Mobile Device operating system built-in security functions (such as user authentication, sandboxes, encrypted per-application storage or any other dedicated application storage which comes with built-in security controls, etc.).

Communication security, encryption:

[HL-SE-08] All communications between the Mobile Application and the Infrastructure as well as in the Federation shall be encrypted. In particular, transport layer encryption shall be used to encrypt data, when communicating over mobile networks and Wi-Fi networks.

[HL-SE-09] All communications in the Federation shall be encrypted.

Cryptography:

[HL-SE-10] Only well-known and publicly recommended cryptographic libraries with well-known and publicly recommended cryptographic algorithms and protocols, and well-tested implementations shall be used.

[HL-SE-11] Special care shall be given to the requirements for the secure use of each algorithm and protocol (e.g. with respect to random or pseudo-random numbers they may use).

[HL-SE-12] Safeguards shall be implemented to prevent relay and replay attacks.

Data Encryption:

[HL-SE-13] The Mobile Application, the Infrastructure and the Federation shall encrypt data as much as possible in order to enhance security and privacy.

Mobile Device built in security:

[HL-SE-14] The Mobile Application shall be secure out-of-the-box (off the shelf) with settings that are secure-by-default.

[HL-SE-15] The Mobile Application shall be designed as intuitive and user-friendly to avoid security issues due to misconfiguration or mistakes by the User.

Risk assessment, incident response:

[HL-SE-16] The Health Authority shall conduct an overall risk assessment focused on the potential cybersecurity risks of a DCTS, taking into account known security issues in the underlying platforms and communication protocols as well as recent incidents and threats.

[HL-SE-17] The relevant parts of the risk assessment shall be shared with the developers of the Mobile Application and the Infrastructure.

[HL-SE-18] Information sharing and collaboration shall be established on cybersecurity and vulnerability management between the developers and the relevant national authorities and bodies, including the national cybersecurity agencies, relevant medical product CSIRT, etc.

[HL-SE-19] Regular threat briefings should be organized as they are an important tool to create awareness of cybersecurity threats at all levels.

[HLSE-20] Plan for incident management and vulnerabilities shall be put in place (before the Mobile Application is deployed), including adequate procedures for the notification and involvement of national CSIRT and relevant cybersecurity and data protection authorities.

Security testing and review:

[HL-SE-21] The Health Authority shall ensure that the security of the Mobile Application and the Infrastructure is reviewed and tested by independent experts with access to all necessary information (including source code), before deployment and after each relevant change.

[HL-SE-22] A procedure for reporting errors and vulnerabilities (by citizens, experts, security researchers, organizations) shall be put in place when the Mobile Application is deployed and adequately publicized.

[HL-SE-23] The Health Authority may also consider further activities to enhance trust such as a bug bounty program.

5.7 Privacy

Temporary usage:

[HL-PV-01] The Mobile Application shall be disabled automatically and all its data stored on the Mobile Device shall be erased, as soon as the epidemic is deemed to have ended by the Health Authority.

Voluntary character:

[HL-PV-02] The installation of the Mobile Application on the Mobile Device and its use shall be based on the consent of the User.

Withdrawal:

[HL-PV-03] The User shall be able to delete or disable the Mobile Application at any time.

[HL-PV-04] When the Mobile Application is deleted all its data stored on the Mobile Device shall be erased.

No location tracking:

[HL-PV-05] The Mobile Application shall not communicate location data to the Infrastructure or any other data that would allow by itself to infer the user location.

Identifiers generation:

[HL-PV-06] The ephemeral identifiers transmitted between Mobile Devices shall neither allow an external party to identify the user of the specific Mobile Device nor to associate multiple signals to the same Mobile Device.

Pseudonyms:

[HL-PV-07] Pseudonyms shall have no relation to long-lived Personally Identifiable Information (PII).

Proximity data on the Mobile Device:

[HL-PV-08] In order to enhance privacy and security, proximity data shall be stored only on the Mobile Device, and be deleted after the epidemiologically relevant period as determined by the Health Authority.

[HL-PV-09] Only after a user has been diagnosed, the proximity data of that user may be uploaded to the Infrastructure and/or made available to the Health Authority.

Data minimization and minimum permissions:

[HL-PV-10] The permissions of the Mobile Application (as granted by the operating system) shall be minimized (i.e. reduced to the strict minimum necessary for its purpose).

[HL-PV-11] The data collected shall be minimized: to the data strictly necessary to perform the intended tasks with deletion of the data that is no longer useful and setting age limits for data retention.

[HL-PV-12] Whenever possible data shall be pseudonymized and/or anonymized.

No stigmatization:

[HL-PV-13] The Mobile Application shall not allow its User to discover the identity of any diagnosed persons or that its User is in close contact with a diagnosed person.

Privacy impact assessment:

[HL-PV-14] The Health Authority shall ensure that the impact of the Mobile Application and the Infrastructure on user privacy is reviewed by independent experts. The experts should have access to all necessary information, before deployment and after each change potentially affecting said privacy. The results of this review shall be made publicly available.

5.8 Interoperability

Epidemiological criteria alignment:

[HL-IO-01] Health Authorities should align with the relevant international organizations (such as WHO and ECDC) on guidance on the determinants of contact tracing for risk calculation, including the definition of close contact (distance and duration of exposure) and the period for data retention for proximity data.

Mobile Application interoperability:

[HL-IO-02] To achieve interoperability between two DCTS a Mobile Application shall record its User's proximity contacts with Users using a Mobile Application from a different DCTS.

Infrastructure in a Federation:

[HL-IO-03] The Federation shall allow to notify, within the delay mentioned in **HL-MA-16**, a User at risk in one of its DCTS that was at risk because of its proximity to a User diagnosed in another of its DCTS.

Diagnosed roaming user:

[HL-IO-04] Data generated by a Health Authority to confirm a diagnosed user shall be recognized and verified by any other Health Authority in the same Federation.

[HL-IO-05] Data entered and generated by another Health Authority to confirm a diagnosed user in a DCTS in the same Federation shall have the same effect as if the data was generated by its own Health Authority.

Annex A (informative): Bibliography

eHealth Network, version 1.0/2020-04-15: "Mobile applications to support contact tracing in the EU's fight against COVID-19 - Common EU Toolbox for Member States".

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

History

Document history		
V1.1.1	April 2021	Publication