ETSI GS E4P 006 V1.1.1 (2021-05)

Europe for Privacy-Preserving Pandemic Protection (E4P); Device-Based Mechanisms for 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

DGS/E4P-006

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

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 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 crisis not limited to COVID-19 by specifying interoperable contact tracing systems.

1 Scope

The present document sets out device based features which pandemic contact tracing systems should meet to ensure their performance and compliance with the ETSI E4P system requirements and interoperability framework defined in ETSI GS E4P 003 [1] and ETSI GS E4P 007 [i.21]. Systems based on a smartphone with cellular and Bluetooth® connectivity will be studied as the first priority and other solutions could be considered later.

In the context of tracing persons potentially infected with a transmittable virus such as SARS-CoV-2, the ISG E4P develops a framework and consistent set of specifications for proximity tracing systems, to enable the development of applications and platforms, and to facilitate international interoperability as defined in ISG E4P Terms of Reference [i.1]. The present document describes device based mechanisms for the Pandemic Tracing Systems.

In particular, the present document specifies various Proximity Detection Methods for Pandemic contact tracing systems, including:

- Proximity detection of contacts
- Anonymous identification of contacts
- Storage requirements for proximity data of contacts
- User experience and usability

Solutions are specified in technical detail so that means of interoperability between different systems and methods can also be readily defined in ETSI GS E4P 007 [i.21] "Pandemic proximity tracing systems: Interoperability framework". Each method is characterized (e.g. in a table) by its degree of compatibility with the ETSI GS E4P 003 [1].

The present document relates to ETSI GR E4P 002 [i.20] "Comparison of existing pandemic contact tracing systems" ETSI GS E4P 003 [1] "Requirements for Pandemic Contact Tracing Systems using mobile devices" and ETSI GS E4P 008 [2] "Back-End mechanisms for pandemic contact tracing systems". In addition, it will be used as an input to ETSI GS E4P 007 [i.21] "Pandemic proximity tracing systems: Interoperability framework".

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 GS E4P 003 (V1.1.1): "Europe for Privacy-Preserving Pandemic Protection (E4P); High level requirements for pandemic contact tracing systems using mobile devices".

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

[3] Bluetooth® Core Specification V5.2.

[4] ETSI EN 301 549: "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] ETSI ISG E4P Terms of Reference (ToR) for "Europe for Privacy-Preserving Pandemic Protection (E4P)", Version 1.1, 8 May 2020.

[i.2] Google API for Exposure Notification - Exposure Notification BLE attenuations.

NOTE: Available at https://developers.google.com/android/exposure-notifications/ble-attenuation-overview.

[i.3] "The Strength of Friendship Ties in Proximity Sensor Data", Vedran Sekara, Sune Lehmann, Published: July 7, 2014.

NOTE: Available at https://doi.org/10.1371/journal.pone.0100915.

[i.4] "Exposure Notification Bluetooth® Specification", v1.2 April 2020, Google Apple.

NOTE: Available at https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf.

[i.5] "Exposure Notification Cryptography Specification", v1.2 April 2020, Google Apple.

NOTE: Available at https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf?1.

[i.6] Decentralized Privacy-Preserving Proximity Tracing GitHub repository.

NOTE: Available at https://github.com/DP-3T/bt-measurements/tree/master/figures.

[i.7] CTIA Test Plan for Wireless Device Over-the-Air Performance, Method of Measurement for Radiated RF Power and Receiver Performance, Version 3.8.1, October 2018.

NOTE: Available at https://api.ctia.org/wp-content/uploads/2019/04/CTIA_OTA_Test_Plan_3_8_2.pdf.

[i.8] Google API for Exposure Notification - Exposure Notifications BLE RSSI calibration procedure.

NOTE: Available at https://developers.google.com/android/exposure-notifications/ble-attenuation-procedure.

[i.9] Android™ API Reference Bluetooth® Low Energy.

NOTE 1: Available at https://developer.android.com/reference/android/bluetooth/le/package-summary.

NOTE 2: Android is a trademark of Google LLC.

[i.10] Apple Developer Documentation Core Bluetooth® Framework.

NOTE: Available at https://developer.apple.com/documentation/corebluetooth.

[i.11] Apple Documentation Archive - Core Bluetooth® Background Processing for iOS Apps.

NOTE 1: Available at https://developer.apple.com/library/archive/documentation/NetworkingInternetWeb/Conceptual/CoreBluetooth_concepts/CoreBluetoothBackgroundProcessingForIOSApps/PerformingTasksWhileYourAppIsInTheBackground.html#//apple_ref/doc/uid/TP40013257-CH7-SW1.

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.

[i.12] PRIVATICS team, Inria, France, Fraunhofer AISEC, Germany, "ROBERT: ROBust and privacy-presERving proximity Tracing, version 1.1", May 31st, 2020.

NOTE: Available at https://github.com/ROBERT-proximity-tracing/documents, https://hal.inria.fr/hal-02611265/en/.

[i.13] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. Le Metayer, V. Roca, "DESIRE: A Third Way for a European Exposure Notification System Leveraging the best of centralized and decentralized systems, version 1.0", May 2020.

NOTE: Available at https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE, https://hal.inria.fr/hal-02570382/en/.

[i.14] J-M. Gorce, M. Egan, R. Gribonval, "An efficient algorithm to estimate Covid-19 infectiousness risk from BLE-RSSI measurements".

NOTE: Available at https://hal.inria.fr/hal-02641630/en/.

[i.15] G. Kessibi, M. Cunche, A. Boutet, C. Castelluccia, C. Lauradoux, D. Le Metayer, V. Roca, "Analysis of Diagnosis Key distribution mechanism in contact tracing applications based on Google-Apple Exposure Notification (GAEN) framework (version 1.2)", September 2020.

NOTE 1: Available at https://hal.inria.fr/hal-02899412/en/.

NOTE 2: https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE.

[i.16] M. Cunche, A. Boutet, C. Castelluccia, C. Lauradoux, V. Roca, "On using Bluetooth®-Low-Energy for contact tracing (version 1.3)", September 2020.

NOTE: Available at https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE and https://hal.inria.fr/hal-02878346/en/.

[i.17] Swiss Confederation, "Replay Attacks", June 14th, 2020, section "Unmasking users by eavesdropping EphIDs".

[i.18] Tijmen Schep, "Corona Detective".

NOTE: Available at https://www.coronadetective.eu/.

[i.19] O. Seiskari, "BLE contact tracing sniffer PoC".

NOTE: Available at https://github.com/oseiskar/corona-sniffer.

[i.20] ETSI GR E4P 002: "Europe for Privacy-Preserving Pandemic Protection (E4P); Comparison of existing pandemic contact tracing systems".

[i.21] ETSI GS E4P 007 (V1.1.1): "Europe for Privacy-Preserving Pandemic Protection (E4P); Pandemic proximity tracing systems: Interoperability Framework".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

diagnosis key: secret code from which ephemeral identifiers for a given period of time can be derived with the help of a cryptographic function

ephemeral identifier: unique device identifier exchanged with another device during a proximity event

proximity event: event recorded by the software on a mobile device corresponding to proximity to other device with an active interoperable application, and which meets the predefined criteria for an event to be recorded (e.g. duration)

3.2 Symbols

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

dB	decibel

3.3 Abbreviations

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

ADV_IND	Advertisement Indication
AES	Advanced Encryption Standard
API	Application Programming Interface
Bluetooth® LE	Bluetooth Low Energy
CID	Content IDentifier
CT	Clearance Time
DB	Device - Backend
DD	Device - Device
DP-3T	Decentralized Privacy-Preserving Proximity Tracing
DPA	Data Protection Authority
DUT	Device Under Test
E4P	Europe for Privacy-Preserving Pandemic Protection
EBID	Ephemeral Bluetooth IDentifier
ECC	Encrypted Country Code
FSPL	Free Space Path Loss
GAEN	Google Apple Exposure Notification
GDPR	General Data Protection Regulation
GR	Group Report
GRX	receiving Bluetooth device antenna gain [dB]
GS	Group Specification
GTX	transmitting Bluetooth device antenna gain [dB]
HKDF	Hashed Key Derivation Function
iOS	iOS Operating System
ISG	Industry Specification Group
ISM	Industrial Scientific Medical band
LE	Low Energy
MAC	Medium Access Control
NTP	Network Time Protocol
PDU	Protocol Data Unit
PET	Private Encounter Token
PRF	PseudoRandom Function
PRG	PseudoRandom Generator
QR	Quick Response (code)
RF	Radio Frequency
ROBERT	ROBust and privacy-presERving proximity Tracing
RPI	Rolling Proximity Identifier
RSSI	Received Signal Strength Indicator
SID	EBID Slice IDentifier
SIG	Special Interest Group
TEK	Temporary Exposure Key
TRP	Total Radiated Power
TRP	Total Radiated Power
TX	Transmit
UD	User - Device
UUID	Universal Unique IDentifier
XOR	eXclusive OR

4 General description

4.1 Reference device architecture

The generic reference E4P device architecture is depicted in Figure 1. It describes a user device and its interactions with other components of the system such as its users, Back-End system (described in ETSI GS E4P 003 [1] as part of the Infrastructure) and other devices. It also introduces three corresponding external reference points and interfaces as follows:

a) **Reference point UD** (User - Device) - User interface.

b) **Reference point DB** (Device - Back-End System) - Back-End interface.

c) **Reference point DD** (Device - Device) - Contact proximity detection interface.

The contact tracing protocols are based on decentralized or centralized design approach as defined in ETSI GS E4P 003 [1]). Based on the model of digital contact tracing system defined in ETSI GS E4P 003 [1], main internal device functions implementing pandemic contact tracing Mobile Application as defined in ETSI GS E4P 003 [1] are described in the following clauses of the present document and are also shown in Figure 1.

NOTE: Optional architecture elements and functions are shown in dotted lines.

These include:

a) **User interface** - describes requirements related to interaction between the user and the device (as defined in ETSI GS E4P 003 [1]).

b) **Contact proximity detection** - describes proximity detection method requirements as defined in ETSI GS E4P 003 [1].

c) **Anonymous contact identification** - describes anonymous contacts identification requirements. This function shall be present in the Device for decentralized approach only as it shall be implemented in Back-End for the centralized approach.

d) **Contact data storage** - describes requirements for data storage and contact tracing protocol between the device and the Back-End. This function may also include Ephemeral IDs generation sub function if it is not implemented in the Back-End.

Detailed architecture of the Back-End system is out of scope of the present document and is described in ETSI GS E4P 008 [2]. High level requirements related to unique device identifiers exchanged on DD interface (Ephemeral IDs) are defined in ETSI GS E4P 003 [1].