ETSI GS E4P 007 V1.1.1 (2021-05)

Europe for Privacy-Preserving Pandemic Protection (E4P); Pandemic proximity tracing systems: Interoperability Framework

ETSI GS E4P 007 V1.1.1 (2021-05)
https://standards.iteh.ai/catalog/standards/sist/10c3576c-8580-4d3b-a609-4e0af3a883d3/etsi-gs-e4p-007-v1-1-1-2021-05

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-007

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 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 digital contact tracing systems.

1 Scope

The present document defines an interoperability framework for pandemic digital contact tracing systems which allows the centralized and decentralized modes of operation to fully interoperate. The present document is part of the ISG E4P specifications describing contract tracing systems and thus aligned with ETSI GS E4P 003 [1]. It is mainly focused on interoperability between ROBERT and DP3T/GAEN, but also contemplates general interoperability mechanisms when more than two protocols can be present in a given geographical area.

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

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

[4] Bluetooth® Core Specification V5.2.

NOTE: Available at https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf.

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 GR E4P 002 (V1.1.1): "Europe for Privacy-Preserving Pandemic Protection (E4P); Comparison of existing pandemic contact tracing systems".

[i.2] "Decentralized Privacy-Preserving Proximity Tracing", 2020.

NOTE: Available at https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

[i.3] Exposure Notifications API.

NOTE: Available at https://developers.google.com/android/exposure-notifications/exposure-notifications-api.

[i.4] "Centralized or Decentralized? The Contact Tracing Dilemma", 2020.

NOTE: Available at https://infoscience.epfl.ch/record/277809.

[i.5] "ROBERT: ROBust and privacy-presERving proximity Tracing", v1.1, May 2020.

NOTE: Available at https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_1.pdf.

[i.6] "On the interoperability of Decentralized Exposure Notification Systems", June 2020.

NOTE: Available at https://arxiv.org/abs/2006.13087.

[i.7] "Interoperable Digital Proximity Tracing protocol (IDPT)", May 2020.

NOTE: Available at https://upcommons.upc.edu/handle/2117/189356.

[i.8] "Herald International Interoperability draft standard", 2020.

NOTE 1: Available at https://vmware.github.io/herald/specs/payload-interop.

NOTE 2: Herald exposure notification solution, hosted by Linux Foundation Public Health.

[i.9] "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://hal.inria.fr/hal-02570382/en/.

[i.10] "Interoperability of decentralized proximity tracing systems across regions", v2.2, 2020.

NOTE: Available at https://drive.google.com/file/d/1mGfE7rMKNmc51TG4ceE9PHEggN8rHOXk/.

[i.11] "European Proximity Tracing: An interoperability architecture for contact tracing and warning apps", 2020.

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

[i.12] "European Interoperability Certificate Governance: A Security Architecture for contact tracing and warning apps", 2020.

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

[i.13] "A state-of-the-art Diffie-Hellman function".

NOTE: Available at https://cr.yp.to/ecdh.html.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

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

dBm	Decibel-milliwatts
KB	Kilo Byte
MB	Mega Byte

3.3 Abbreviations

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

4G	Fourth generation of broadband cellular network technology
5G	Fifth generation of broadband cellular network technology
API	Application Programming Interface
app	Application
BCGL	Backend Certificate Governance and Lifecycle
BF	Back-end to Federation
CC	Country Code
CH	Confédération Helvetique
COVID-19	COronaVIrus Disease 2019
DCT	Digital Contact Tracing
DCTS	Digital Contact Tracing System
DH	Diffie-Hellman-Merkle
DP3T	Decentralized Privacy-Preserving Proximity Tracing
EBID	Ephemeral Bluetooth® IDentifier
ECC	Encrypted Country Code
EFGS	European Federation Gateway Service
EphID	Ephemeral IDentifier
EU	European Union
FGS	Federation Gateway Service
GAEN	Google Apple Exposure Notification
GATT	Generic ATTribute Profile
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
ID	IDentifier
IDPT	Interoperable Digital Proximity Tracing
IO-C	InterOperability Challenge
JSON	JavaScript Object Notation
LE	Low Energy
LTE	Long Term Evolution
MAC	Medium Access Control Address
MTU	Maximum Transfer Unit
OS	Operating System
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
RI-ECC	RI Encrypted Country Code
ROBERT	ROBust and privacy-presERving proximity Tracing
RSSI	Received Signal Strength Indication
SIG	Bluetooth® Special Interest Group
TLS	Transport Layer Security
TV	Television
TXpower	Transmitted power
UK	United Kingdom
UTF	Unicode Transformation Format
UUID	Universally Unique IDentifier
UWB	Ultra-Wide Band

4 Interoperability challenges

4.1 Overview

This clause discusses the challenges that appear for achieving interoperability between different DCTSs. As discussed in clause 4.1 of ETSI GR E4P 002 [i.1], DCTSs aim at providing an automated, privacy-preserving method of detecting potential contagion and warning people to apply for screening. The aim of interoperability is to make possible this functionality for people using different DCTS apps which, for instance, have been developed by different public authorities.

The main requirements related with interoperability are the following; see clause 5.11 of ETSI GS E4P 003 [1]:

- [HL-IO-01] Epidemiological criteria alignment;
- [HL-IO-02]: Mobile Application interoperability;
- [HL-IO-03]: Infrastructure in a Federation; and
- [HL-IO-04], [HL-IO-05]: Diagnosed roaming user.

Regarding the reference device architecture defined in ETSI GS E4P 006 [2], the main involved reference points are:

- reference point DB (Device - Backend System) - Backend interface; and
- reference point DD (Device - Device) - Contact proximity detection interface.

While for the reference backend architecture defined in ETSI GS E4P 008 [3], the main involved reference point is:

- Reference point BF (Federation Interface).

Clause 4.2 discusses Bluetooth® LE implementation challenges: Standards compliance, functional breadth, and reliability of low-level protocols like Bluetooth® on consumer systems that were designed for accessories like Bluetooth® audio, and not accurate medical risk estimation or contact tracing applications.

Clause 4.3 discusses the interoperability challenges for digital contact tracing protocols. The main contact tracing protocols developed so far are based on decentralized or centralized design approaches, as defined in ETSI GS E4P 003 [1]. The protocols that will be covered in the present document are:

- DP3T/GAEN: the version of the DP3T decentralized protocol specified in [i.2] which is based on the use of the GAEN API [i.3]; and
- ROBERT: the centralized protocol specified in [i.5].

ETSI GS E4P 006 [2] describes a third protocol, DESIRE, that can operate following either centralized or decentralized approach; see [i.9]. However, interoperability aspects for this protocol are not covered in the present document.

Clause 4.4 examines the challenges of keeping the same privacy characteristics of the DCTS when they work in stand-alone in case of interoperability, while clause 4.5 briefly discusses the problem that could arise in terms of amount of exchanged traffic when many users of DCTS interoperate. Clause 4.6 briefly discusses the interoperability challenges that appear when different DCTSs that use different risk scoring algorithms, although a detailed description is left out of the scope of the present document. Other challenges to interoperability not covered in the present document are:

- Access to technology (e.g. handsets, wearables) and network access (Internet) varies greatly according to geography, income, and community. Supporting only the latest handsets denies poorer and more at-risk communities access to this technology.
- Governments may take different decisions on approach based on local needs. These decisions have, by necessity, been taken independently with urgency. This includes different risk appetites and approaches for individual privacy and national security.

Clause 5 is devoted to discuss the interoperability between the device-to-device payload exchange protocols used by different DCTSs. Clause 6 is devoted to the case when the DCTS use the same design approach, while clause 7 discusses the interoperability when the design approach of the involved DCTSs is different. This distinction is necessary as the interoperability challenges are considerably different in the two cases. The main problems of interoperability between DP3T/GAEN and ROBERT appear due to the different privacy properties of these two protocols; see clause 7.2 of ETSI GS E4P 008 [3]. A direct interoperation between them would lead to major changes in privacy properties for some of the users in relation with standalone systems, as discussed in clause 7.1. A solution that implies some modifications in the protocols, but that preserve the privacy properties of the different systems is discussed in clause 7.2.

Finally, clause 8 discuses interoperability between the device-to-device payload exchange protocols when more than two protocols need to be supported.

4.2 Bluetooth® LE Interoperability challenges

4.2.1 Introduction

If two systems are using different Bluetooth® LE advertisement modes, the related applications might not be able to share data and trace contacts when at proximity.

If two systems are using the same Bluetooth® LE advertisement modes, but a different Bluetooth® LE payload, the related applications might not be able to understand each other data and trace contact when at proximity. This is discussed in detail in clause 5 of the present document.

4.2.2 Bluetooth® LE mode to advertise and scan

The applications of two different DCTSs could use different advertisement modes, as presented in clause 5.1.2 of ETSI GS E4P 006 [2].

The applications should be capable of using the different mode of advertisement described in in clause 5.1.2 of ETSI GS E4P 006 [2].

4.2.3 Bluetooth® LE Advertisement Payload

The applications of two different contact tracing systems could use a different payload as described in clauses 5.2.1.1.1 and 5.2.2 of ETSI GS E4P 006 [2].

It is recommended that all applications are using the same payload format and content. If not, the applications should be capable of sharing and understanding the different payload described in clauses 5.2.1.1.1 and 5.2.2 of ETSI GS E4P 006 [2].

If two applications use the same payload content and format, they should use the same UUID as described in [4].

If two applications do not use the same payload content and format, they should use a different UUID.

For instance, the UUID and payloads contents of the application used in France and in Germany are different. The UUIDs are respectively 0xFD64 in France and 0xFD6F in Germany; the payloads contents are also different as different protocols are used.

4.2.4 Bluetooth® standard versions in use

Since its introduction in 2010, Bluetooth® LE has gone through several versions, each introducing additional modes and features. Using the latest Bluetooth® 5 protocol and its security features would mean a large proportion of the population could not access the benefits of DCTS applications. Many wearable and embedded chips used for DCTS applications may also only support older standards such as Bluetooth® LE 4.0 and 4.1.

It is recommended that DCTS applications ensure their protocols can be used back to Bluetooth® LE 4.0.

4.2.5 Bluetooth® hardware support for advertising

Many phones' use of Bluetooth® is limited to accessing external peripherals such as speakers and car hands free kits. They were not designed primarily to act themselves as peripherals. This means many Bluetooth® chipsets, whilst technically capable of being used for advertising, do not have the firmware necessary to provide these services to the host operating system. During 2020, handset manufacturers have improved firmware, but these updates may not be widely applied in existing handsets without automatic updates enabled.

The implication of this is that an advertising only protocol may not allow certain devices, even though they may have been produced in the last 2 years, to be 'seen' and recorded as a contact in a DCTS application.

4.2.6 Operating System Bluetooth® compliance

Many parts of the Bluetooth® standard are optional. As mentioned in the previous clause the use of phones in both central and peripheral modes was not a common use before 2020. As a result, mobile phone OS' support varies for certain parts of the standard.

These challenges start from the modes of advertising (passive, active, etc.) and scanning (continuous with callbacks, or duration based), extend through the handling of connection sessions (e.g. expecting interactions between devices being serial in terms of request/responses, and stalling and timing out if this may not occur), characteristic modes supported (e.g. no write without response) and finally to the handling of data exchanges (e.g. fixed MTU, buggy MTU negotiation on Android).

All of these variations from the standard require specific handling or a reduction in the number of Bluetooth® features that can be relied upon with which to implement a device-to-device protocol and payload exchange over Bluetooth®; see clause 5.

4.2.7 Accessing information necessary for accurate contact detection and risk calculation

Much research has occurred in 2020 in to distance estimation, and thus risk estimation, based on Bluetooth® RSSI data. In order to best correct these estimations, it is not only needed to know the local RSSI for the remote device, but also ideally the phone make and models for each device, and the transmit power of the remote advertising device. Some of this is present in the clear via Bluetooth® standard services but is not always present across all phones and mobile operating systems' Bluetooth® advertisements.

4.3 General challenges related to the functional requirements

4.3.0 Satisfying requirements for interoperability

One of the main interoperability requirements is functional requirement HL-IO-03, which is repeated here for convenience:

- **[HL-IO-03]:** Functionality in a Federation: The Federation shall allow to notify, within the delay mentioned in Timing of notification of users at risk, a User at risk in one of its DCTS that was at risk because of its proximity to a User tested positive in another of its DCTS.

Satisfying requirement HL-IO-03 is challenging even across DCTSs with a common design approach (see clause 6) and even more challenging across those with different design approaches (clause 7). Conceptually, a high-level solution to this requirement differs depending on whether a User that tested positive (Diagnosed User) is located in their home country at the time of proximity event (i.e. the User is a Local) or in their roaming country at the time of the proximity event (i.e. the User is a Traveller). Therefore, the two Users in HL-IO-03 can be two Locals, a Local and a Traveller, and two Travellers. As the case of the proximity encounter of two Locals is not an interoperability challenge as it needs to be solved by any individual DCTS, the focus is put on the remaining cases.

Consider first the case of proximity encounter of a Local and a Traveller. Two different cases should be distinguished:

1) the case where the Diagnosed User is a Traveller and a User to be notified is a Local; and

2) the case where the Diagnosed User is a Local and a User to be notified is a Traveller.

4.3.1 Notification to a Local about a diagnosed Traveller

This case is depicted in Figure 1. Alice lives in country A. Alice gets in proximity of a Traveller, Bob, who could be from any country in the world. Bob returns to his country B two days later and is tested positive. Alice, aware of Bob's symptoms, is concerned she might be infected, too. How does Alice learn about Bob's infection, without being a User of all DCTSs in the world?

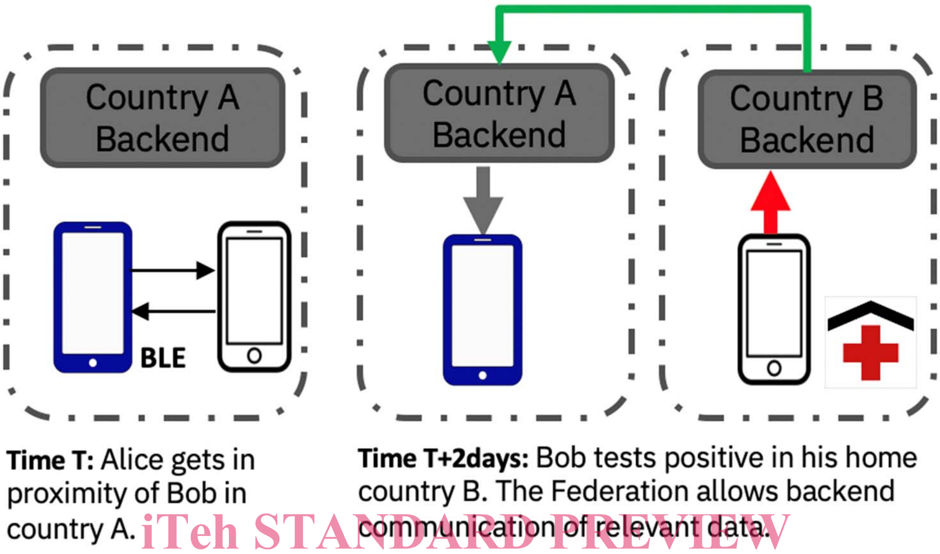

Figure 1: Local Alice infected by traveller Bob

The first case to be considered appears when the system includes geographic information in the exchanged beacons, as it is the case of ROBERT. In this system, the beacons include an Encrypted Country Code (ECC) of the sender of the beacon. In ROBERT, the system exchanges exposed anonymous identifiers, meaning that Bob will include the beacons received from Alice in the list of exposed keys uploaded to the Country B backend when he notifies a positive test to the app. The Country B backend should have thus a method for de-crypting the ECC contained in the beacons of Alice, to known to which server it should relay Alice's exposed keys.

The second case appears when no geographical information is included in the exchanged beacons, as is the case of DP3T/GAEN. Notice that the main issue here is that Alice has no idea from which country Bob comes from. Clearly, it is unfeasible for Alice to install all possible Mobile Applications pertaining to every DCTS. Even if Alice's and Bob's countries use DCTSs with the same mechanism, it might be impossible for Alice to unselectively listen to all backends from all countries due to sheer volumes of data. For instance, assuming an scenario in which 300 000 daily COVID-19 infections are notified in the world using a federated DP3T/GAEN system, every user would need to download more than 70 MB of data daily; see [i.6].

Instead, if Diagnosed Users would upload some coarse-grained travel/roaming information to backends, this information would be very helpful to improve scalability of the Federation. For usability and privacy requirements, the information about visited countries should not be fine grained. There are two options in this case:

- Partial replication, on a need-to-know basis, across a majority of countries. In this case, Bob would inform the Federation (starting from country B backend) about the fact that he visited country A. This would allow Federation to propagate critical information from country B to country A.

- All-to-all replication, across a cluster of affiliated countries (e.g. EU countries). In this case, Bob would not need to upload his travel information to country B backend, but all data would be replicated across all backends belonging to a cluster.

Consequently, interoperable backends of DCTSs, comprising the Federation, shall be able to communicate with each other in a secure and authenticated manner and disseminate critical information among each other.

4.3.2 Notification to a Traveller about a diagnosed Local

If the system includes geographic information in the exchanged beacons, as it is the case of ROBERT, the situation is identical as in the previous clause.

In the case of a solution without geographical information exchanged in the beacons, as it is the case of DP3T/GAEN, and conversely to the case described in the previous clause, if Alice (Local) gets infected, there is no way she could direct the diagnosis information to be propagated from country A backend to country B backend (recall that Alice has no idea where Bob comes from). As global all-to-all replication involves prohibitive volumes of data, the Federation needs to allow Bob to listen to information coming from country A backend; see also illustration in Figure 2. In this case, Bob knows to which country backend to listen, as he knows he travelled to country A.

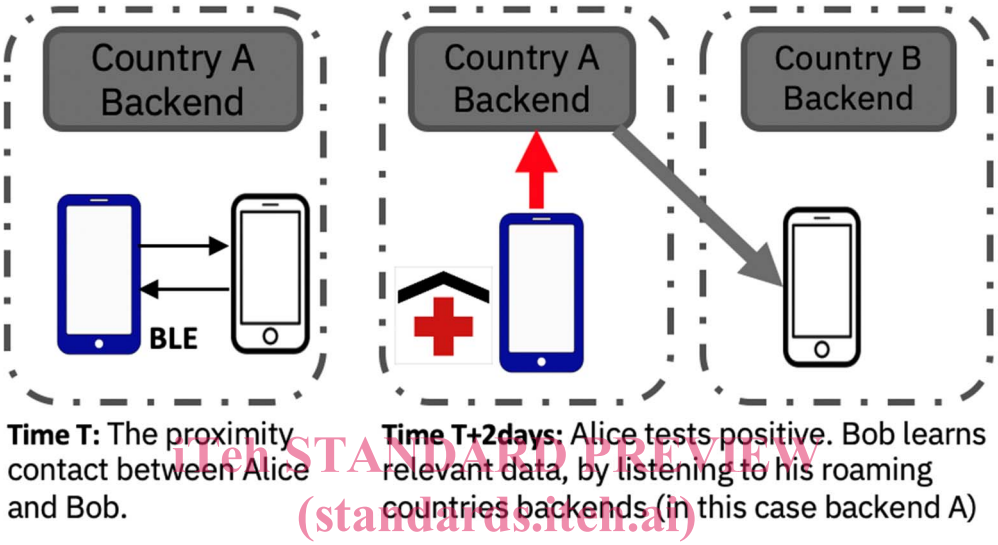

Figure 2: Traveller Bob infected by Local Alice

In a cluster of country backends, which perform all-to-all replication, as discussed in clause 4.3.1, Bob may get relevant data directly from backend B.

4.3.3 Notification to a Traveller about a diagnosed Traveller

If the system includes geographic information in the exchanged beacons, as it is the case of ROBERT, the situation is identical as in the previous clauses.

In the case of solution without geographical information exchanged in the beacons, as it is the case of DP3T/GAEN, it is fairly easy to show that a Federation system which solves challenges described in clauses 4.3.1 and 4.3.2 can also solve this challenge.

4.3.4 Authenticity of positive test information in case of a roaming User

Clause 4.3.1 discussed the case in which Bob gets tested positive in his home country B. The situation changes if Bob is tested positive in country C (different from B). Assuming that Bob cannot reach his home country B (in which case solution outlined in clause 4.3.1 would apply), the Federation needs to allow Health Authorities of country B accept positive test results of country C so Bob is allowed to upload relevant diagnosis data to country B backend.

Assuming Federation requires Bob to upload relevant diagnosis data to country B backend upon Bob tests positive in country C, this requirement can be satisfied leveraging a Verifiable Credentials standard compatible solution, which could be implemented on a decentralized verifiable credentials platform, such as a permissionless or permissioned block-chain. In a nutshell, in such a solution, public certificates of health certificate issuers (Health Authorities) are stored on the decentralized verifiable credentials platform (with no information pertaining to Users being stored on the said platform).

Alternative approach would be to require Bob to upload relevant diagnosis data to country C backend. However, this approach would pose serious operational and implementation problems as mobile applications are normally capable of communicating with the home backend of that application, not with an arbitrary roaming backend.

4.4 Maintaining privacy and security characteristics between different systems

The proposed digital contact tracing protocols can be vulnerable to several potential attacks to privacy and security; see clause 7 of ETSI GS E4P 008 [3]:

- Risk of obtaining the identity of a user from the knowledge of the ephemeral identifiers (i.e. the possibility of tracking people).
- Risk of disclosing the graph of contacts of users.
- Risk of identification of infected people. All digital contact tracing methods are vulnerable to this attack for individual users. Large-scale attacks are a potential vulnerability of some of the methods.
- Risk of injection false at-risk alerts.
- Risk of being pressed to opt-in.

One challenge for interoperability is to ensure that the DCTS interoperability infrastructure shall retain, to the extent possible, the security and privacy provided by individual DCTSs.

This is especially difficult to achieve when the interoperability between systems with different mechanism is considered, as they can have very different properties regarding privacy and security; see clause 7.

4.5 Generated traffic

As discussed in clause 4.3.1, interoperability across different DCTSs imply that some information is exchanged between backend servers supporting different DCTSs. Depending on the adopted architecture (e.g. all-to-all or partial replication) the amount of exchanged traffic can be substantially different. This is an important factor to be taken into account when interoperability across DCTSs with many users (potentially, billions of users) is aimed.

4.6 Interoperability between DCTS applications

The present document mainly deals with technical aspects of DCTS interoperability. There are, however, other aspects that are key to achieve interoperability between DTCS applications, for instance:

- Harmonization between countries of procedures to request tests, to obtain and enter authorizations to release proximity events.
- Criteria and algorithms used to record proximity events, and the way proximity events are structured and handled in the DCTS app.

The DCTS apps should be able to record significantly more events than would be found with manual contact tracing, which requires the '15/1.5' style criteria to be abandoned; furthermore, that two sets of criteria are used for proximity events, with:

- one set for recording events;
- the second set for selection of events for uploads.

This would allow events to be recorded for the benefit of the user (mapping recorded encounters per day, per week, to give the user an idea of possible risks) and for research, while the number of proximity events used to generate warnings could be controlled separately.

Finally, multiple sets of criteria could be loaded, where each set would correspond to the criteria to be used for a certain region or risk level that could be coupled to regional indications by the mobile operators.

This could be realized as follows:

- use agreed, much more sensitive values for the pair time/distance parameters: suggested is 3 minutes/2 meters; or