Horizon 2020 ETC 636126

D 4.1 Privacy Reference Design

A Generic Framework for Open Account-Based Travelling

February 13th 2017

Version 1.0 FINAL

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 636126.

Any dissemination of results reflects only the author's view. The Agency is not responsible for any use that may be made of the information it contains.

Contents

1 Introduction & Summary

This document is Deliverable 4.1 Privacy Reference Design and is part of work package 4 '*Define & Plan for the Traveller-in-Control Privacy Solutions*'.

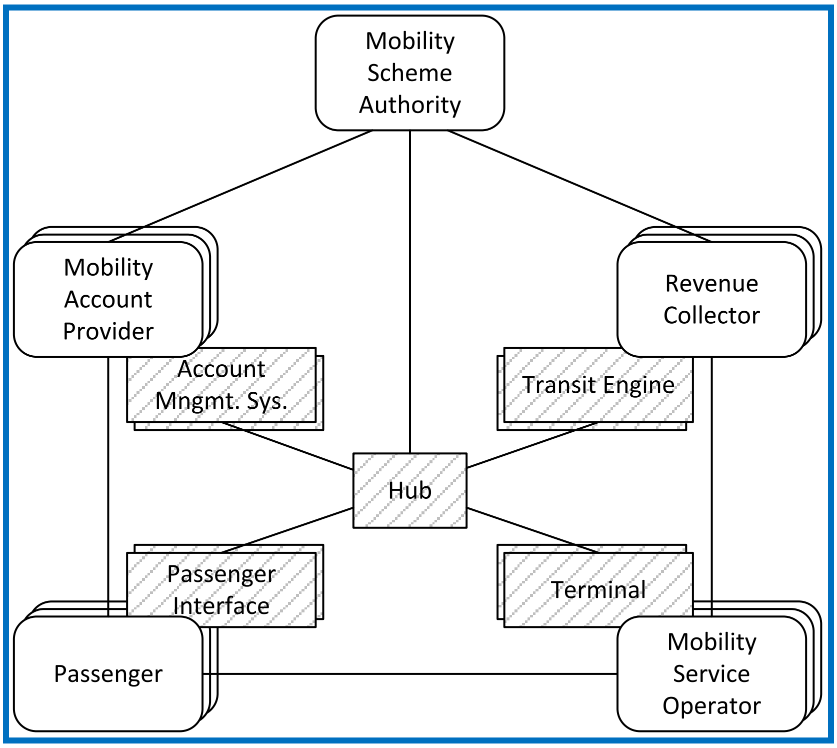
The goal of the Privacy Solution of the European Travellers Club (ETC) is to maintain a relation based upon long-term trust from both its travellers as its traveller organisations. In this document a further detail of this goal is presented, towards the creation of a *Reference Design* that should be included in the implementation of the core systems of the ETC and its members.

2 Goal of the ETC regarding privacy

2.1 Main goal and objectives

One of the **main goals** of the ETC is to maintain long-term trust from its travellers and its traveller organizations. This goal will be part of the technical systems as well as the governance of the ETC, which means that we will define a Reference Design which is to be used within the design of our systems as well as in the design of our ETC member schemes and in the set-up and governance of the not-for-profit entity: the European Travellers Club. This design should protect the traveller, as owner and subject of the data, from insecure system design. Furthermore, the privacy solution should incorporate user experience design to ensure that the use of the product is intuitive in design and simple in operation (see also chapter 4 of this document).

We believe that it is necessary and crucial that travellers are put in control of their 'own' data and also that it is necessary to avoid anti-competitive behaviour of players within our eco-system. We have described the eco-system and its players within work package 3 (see picture below).



There will be a Scheme Authority that defines the scheme roles, rules and interfaces, and may facilitate the routing of transactions between various players. Important part of these rules will be the privacy related rules. The central systems of the ETC are described in work package 6, in which privacy and trust are conditions to explore and describe a trust-framework for the ETC members in which they can trust the accounts of travellers with third party agencies, including those from other countries or regions, without the need to sign up such customers themselves.

The systems to be used by other relevant parties are described in work package 8 and 9.

The **specific objectives** of this work package 4 '*Define & Plan for the Traveller-in-Control Privacy Solutions*' are:

- to select technologies and develop processes that give travellers full control of and direct access to their profile and transaction data, while limiting the data that any service provider can collect on an individual customer to only those transactions with that specific service provider for which the customer has agreed to be known; and

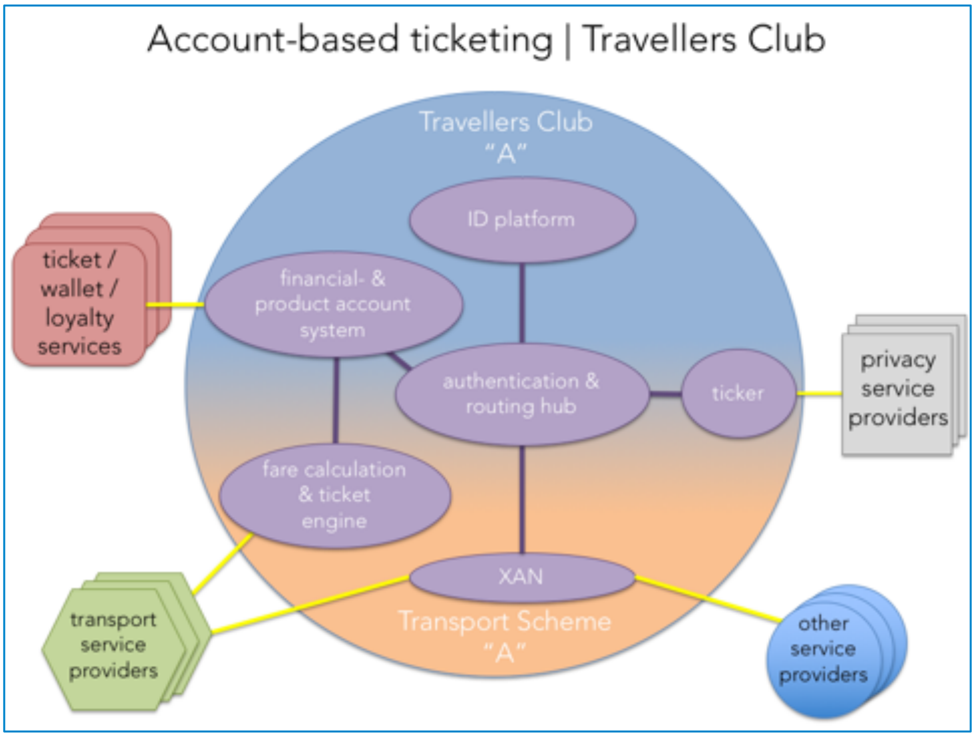
- develop the Requirements, Standards and Audit Procedures for the implementation of next-generation privacy concepts that each national or regional Travellers Club will have to adhere to, including:

2.2 High-level requirements

The ETC envisages the following high-level requirements regarding privacy:

1. separation of roles, between an Identity Platform and various service providers, with derived identities per service provider (see also picture below).

2. traveller-in-control, meaning that:
    - ○ the traveller remains the owner of all profile data, and decides what profile data is to be shared with which service provider (not every service provider needs to know the identity of its clients), and
    - ○ all transaction data from every service provider is fed back to the traveller, who can decide on its storage and use by third parties.


Account-based ticketing | Travellers Club
Travellers Club "A"
ID platform
financial- & product account system
authentication & routing hub
ticker
fare calculation & ticket engine
XAN
Transport Scheme "A"
ticket / wallet / loyalty services
privacy service providers
transport service providers
other service providers

2.3 Possible future requirements

Next to above mentioned requirements the ETC also focusses on 2 other requirements. These have not yet been included, but could be part of future requirements. We will discuss these further with travellers and representatives (like the European Passengers Federation), to identify its relevance and if the ETC is ready for these requirements.

1. private Data Vaults in which a traveller can store his or her own data securely, and – for the future – Zero Knowledge Data Storage, in which that data is stored in a distributed, anonymous and encrypted way, such that a third party cannot reconstruct the data without approval of the traveller.

2. privacy Service Management, as a separate role, to translate third party data requests into executable proposals to Travellers in the most privacy- friendly way.

3 Implementation - governance

3.1 Market Imperfection

As stated in chapter 1, it will be the role of the Scheme Authority to set the rules for privacy. We have recognised that ‘privacy’ is one of the current market imperfections[1]: “*Some service providers aim to use transaction and personal data of their users for commercial purposes*.”

We need a new approach towards the end user of the system, the traveller to solve this market imperfection. This new approach should focus on providing service, but without losing the trust of the customer (or traveller). Currently both commercial companies as well as (transport) authorities experience that this trust can no longer be maintained on the basis of promises and security. We furthermore have identified that if you would provide additional (transport related) services to travellers, privacy becomes even more important. So we have concluded that that privacy should be embedded in the design of the system and governance and that the traveller should be in control of her or his own data.

The ETC with existing e-ticketing schemes can make a significant contribution to solving the market imperfections, also the privacy related imperfection: “*… the transport ticketing schemes already operate in the public domain and make no commercial use of travellers’ data.*”

We therefore have agreed with the (future) members of the ETC that requirements regarding privacy within the e-ticketing system will be part of the scope of the ETC as the envisaged Scheme Provider, or authority.

3.2 Guiding Principle

As guiding principles for privacy we have defined:

1. separate profile data from transaction data. In other words: the identity platform does not store any transaction data.

2. provide transaction data to service providers only on “derived identities,” so that service providers cannot build a complete profile of the travellers.

3. only travellers are in the position to combine all their data in their own data vault, where they can decide how long they wish to store which kind of data and what kind of analyses they allow to be performed on that data.

The guiding principles can be captured in our view regarding the traveller:

> **Put the traveller first**. All decisions affecting Travellers need to be evaluated from the perspective of the Traveller; where possible Travellers must be in control of their own data; the participation of Travellers or their representatives in the governance structure is actively promoted.

[1] See Deliverable 3.1.

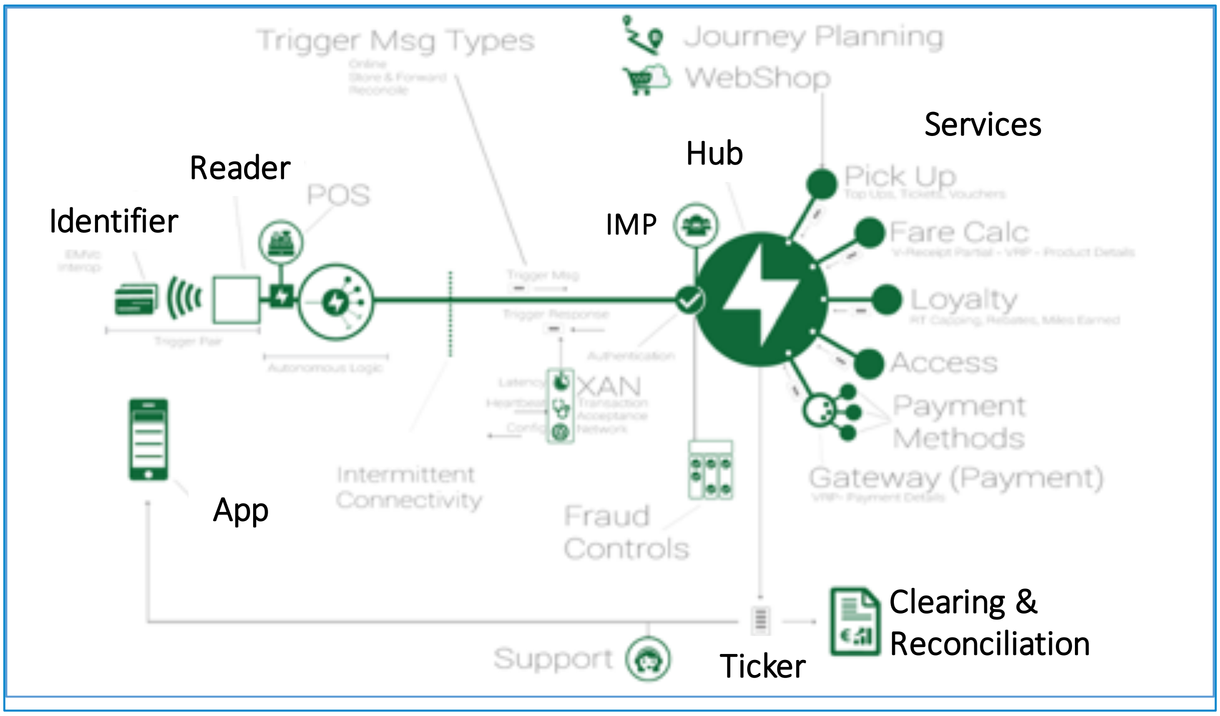
3.3 European Passenger Federation

The ETC has asked the representative of the traveller, the European Passenger Federation (EPF), to act as an advisory body to the European Travellers Club. We envisage a workshop(s) with the EPF to discuss the high-level requirements and guiding principle regarding privacy.

4 Implemenation - technical

4.1 ETC Architecture

The overall and high-level architecture of the ETC is presented below:



The foundation of any Account Based Ticketing (ABT) platform is the ‘Account’. This user account supports both anonymous accounts and rich profile building for personalized accounts with automated field level verification of key fields e-mail, mobile number, bank account, home address so that these may be used for delegated authorization with external parties via opt-in.

4.2 Technical – high-level – requirements for the Identity Management Platform (IMP)

The Identity Management Platform (IMP) is part of the eco-space of the ETC, see picture above. This platform will have the possibility to integrate with member schemes (single sign on) and create accounts.

For the IMP there should be an identity vault with Opt-in controls. The following requirements have been set:

1. hashed salted password storage,
2. encrypted storage of personal profiles,
3. high value service tokens used for bank access,

4. a privacy wall for communication with third party services via proxy accounts and proxy tokens (derived Token IDs),

5. user managed opt-in controls for sharing of personal data with ancillary services.

4.3 Design requirements for member schemes

Above stated requirements for the central systems of the ETC will – as a next step – be discussed with (future) members of the ETC.

Draft design requirements for member systems:

I. Meet new customer expectations and respect privacy, eg.
   - single consumer (traveller) app for door-to-door journeys. Choice of apps, at least one from member scheme (or transport authority);
   - easy and single on-boarding for all services;
   - personal preferences and customer-controlled Privacy;
   - etc.

II. Integrate Private and Public Transport

III. Enable new players and innovation

IV. Operate across borders

4.4 Shifts when introducing ABT

When introducing ABT in an e-ticketing scheme the ETC envisages that there will be a shift towards the so-called *trusted traveller*. Two important aspects of this shift are: (1) the shift from ticket to relation; and (2) the shift from revenue protection to service.

Ad 1. From Ticket to Relation. When ABT is introduced in an e-ticketing scheme the scheme should be aware of the following: (a) a known-customer can be offered a better, tailor-made service; and (b) a known-customer can be offered more courtesy in revenue protection. Either because “I” know and trust the customer, or because she is trusted by another account-provider whom I trust (e.g. another member scheme of the ETC). But customers should be able to travel anonymous, delete data, and opt-out of service offerings!

Ad 2. From Revenue Protection to Service. To influence behaviour of travellers the scheme will have to inform and incentivise. In order to do this effectively we need people to accept, like it and use it. In order to reach that we need to: (a) provide the best value and experience; and (b) be trustworthy (with respect to security, privacy and customer-control).

Another important shift is the shift from ticketing to *travelling*. Three important aspects of this shift are: (1) planning and booking of a trip or journey is added; (2) access and inspection can be done at a more customer friendly way; (3) disruptions and changes can be handled in a more customer friendly way; and (4) offerings and advice can be more customer friendly.

Ad 1. Planning and booking is added. Multi-modal journey planners with clear options can be added (see also work package 9 for this). The usage of these apps can be simplified through the use of personal preferences and be more pro-active through the use of historical data. One-click booking (but with flexibility) can be added and also advises with respect to notifications (where is the bus stop, bike availability, which identifier to use etc.).

Ad 2. Access and inspection. Access and inspection can be done at a more customer friendly way. If the traveller is known, inspection does not lead to confrontation but to notification via the app: e.g. *"please top-up your online wallet, or buy a ticket (and store it online)*." Identification can be an electronic token (card or mobile), optical (barcode) or even personal (as with Uber).

Ad 3. Disruptions and changes. Predefined journeys allow for warnings before journey, or a leg of a journey, is undertaken. The service provider can offer alternatives or compensation. The customer can decide to stop or alter the journey.

Ad 4. Offering and advice. Back-Office based offerings can be updated easier (e.g. free use of buses on a national holiday). Travellers who use the planner can be offered all options, including door-to-door journey times and costs. Travellers with an account can be offered best-price guarantees (eg through daily or weekly capping). Travellers with known histories can be offered targeted incentives to change behaviour. Future: with access to their agenda's, travellers can receive prospective advice and notifications

Finally, we have identified the shift towards a so-called *open architecture*, with the following aspects: (1) multi-modal travelling; (2) multi-functional interaction; and (3) cross border acceptance.

Ad 1. Multi-modal travelling. The transaction network has to be able to work with multiple transport modes, while maintaining a positive customer experience, and consistency with planning and offering.

Ad 2. Multi-functional interaction. To be more relevant to the user (e.g. access to schools, municipal services etc.) and to be more cost-effective (more transactions via the same infrastructure).

Ad 3. Cross border acceptance. Cross border acceptance, at least for the account, preferably also for travel apps and identifiers, with a need for travelling abroad and allowing foreigners travelling in your scheme. This requires trust between schemes / account-providers, a routing infrastructure between schemes (via the ETC interoperable hub) and a standard transaction settlement format.

When designing the system and implementing the privacy requirements and guidelines, these shifts (aspects) needs to be taken into account.

5 Next steps

5.1 Governance

The ETC will be set up as a not-for-profit entity. Part of the governance of the ETC will be an advisory role of the European Passenger Federation (EPF). With this, travellers representative organisation we will organise workshop(s) in order to further design the privacy aspect of the ETC. This will have an effect on the statutes of the ETC, membership agreements, franchise contracts etc.

5.2 Technical

Within the definition of the central systems of the ETC, the privacy requirements have been taken into account. The ETC will discuss further – in workshops – with its (future) members how these privacy requirements should be implemented in their systems as well.