Integrated Identity Management for
Travel, Migration and Security in Europe

I. Abstract

Given the challenges that the EU faces in terms of crises and the influx of refugees, it is of utmost importance to share information in the fields of travel, migration and security. New efforts must be made to fix the existing flaws in the information-sharing process at EU level. These flaws are not the result of a lack of systems or institutions. Instead, existing information resources and channels must be strengthened, connected and used more actively. Multiple collection, registration and storage of personal data should be avoided. Avoiding redundancies leads to better data quality and data minimization, which is imperative in terms of both security and data protection.

In the EU, different systems are currently used to register data related to travel, migration and security (Eurodac, VIS, SIS, Prüm, API). There are plans to launch new systems (PNR, Smart Borders). The European Agency for Large-Scale IT Systems, eu-LISA, has been established to operate those systems that are based on central procedures (Eurodac, VIS, SIS) or future systems (Smart Borders; service provider for PNR, if necessary). Other systems (Prüm, PNR, API) are decentralized by design so that, for member states, overall access to information is more difficult, not possible at all or possible only in certain legal circumstances when additional steps to match information have been taken.

However, central data systems are not compatible with each other. As a result, information that is collected for the same or similar purposes or even contains largely the same data cannot be combined. This may lead to blind spots in Europe's security architecture.

Integrated solutions for entry and exit checks and travel into, out of and within the Schengen area are therefore necessary. Just like in the field of e-government, the once-only-principle should also be consistently applied and legally, operationally and technically implemented in the field of public security to ensure practical operability (no obstruction of travel of bona fide travellers; no restriction of the freedom of movement; better data quality by avoiding redundancies) and data minimization (the same data should not be collected twice).

II. Current situation

At EU level, there are currently five systems and tools that are also intended to check third-country nationals entering or staying in the Schengen area. Legal acts for two more EU systems intended to collect, store and process information on travellers are being prepared at the moment.

1. Multiple collection of the same information

Certain basic data (alphanumeric data such as name, first name, etc. and biometric data such as fingerprints) are collected separately for each system. This is not in line with the data protection principle of data minimization. Storing the same information multiple times increases the risk of errors and insufficient data maintenance and, as a result, leads to poor data quality. Multiple data collection makes processes more complex, slows them down and increases costs – to the detriment of the authorities collecting data and the travellers concerned who are especially interested in swift and smooth procedures. Especially in terms of border crossings, the first control line is highly time-critical; manual data collection must be kept to a minimum.

2. No information networks

Since information is stored separately (in a silo-like manner), it is not possible to recognize connections quickly and reliably. Authorities *do not know what they know*. It is not possible for them to create an overall picture by combining individual data fragments. Especially when it comes to dynamic migration movements (e.g. during the current refugee situation), available information is combined only in a fragmented, delayed and rather accidental manner, which creates dangerous knowledge gaps.

3. No flexibility

As a result of the silo-like information architecture, every system discussed here is a complex large-scale IT system. It is extremely expensive to set up and operate such systems. From a technical perspective, synergies cannot be realized. Adding (or removing) individual elements requires a comprehensive re-design. Implementation processes take years and make it impossible to respond to new challenges in a flexible way.

These redundancies are also of operational, legal and political character. The same discussions (e.g. on the registration of biometric characteristics, access requirements for security authorities) take place repeatedly, lead to a distorted political and public

perception and often result in unrealistic restrictions that considerably limit the practical use.

III. Corrective

To counteract the fragmentation of the European system landscape and the multiple collection of the same data, this approach seeks to combine the relevant systems in an integrated identity management for travel, information and security.

1. Objective

According to the principle of modularity, the systems will be combined in an integrated system architecture.

- The core module will contain the basic data on the traveller (i.e. alphanumeric and biometric data).
- Other information and specific features of the different systems (e.g. visa data, PNR) will be stored in specific modules.
- The core module and the specific modules are connected with each other so that the respective data sets are linked in such a way that they provide the required information.

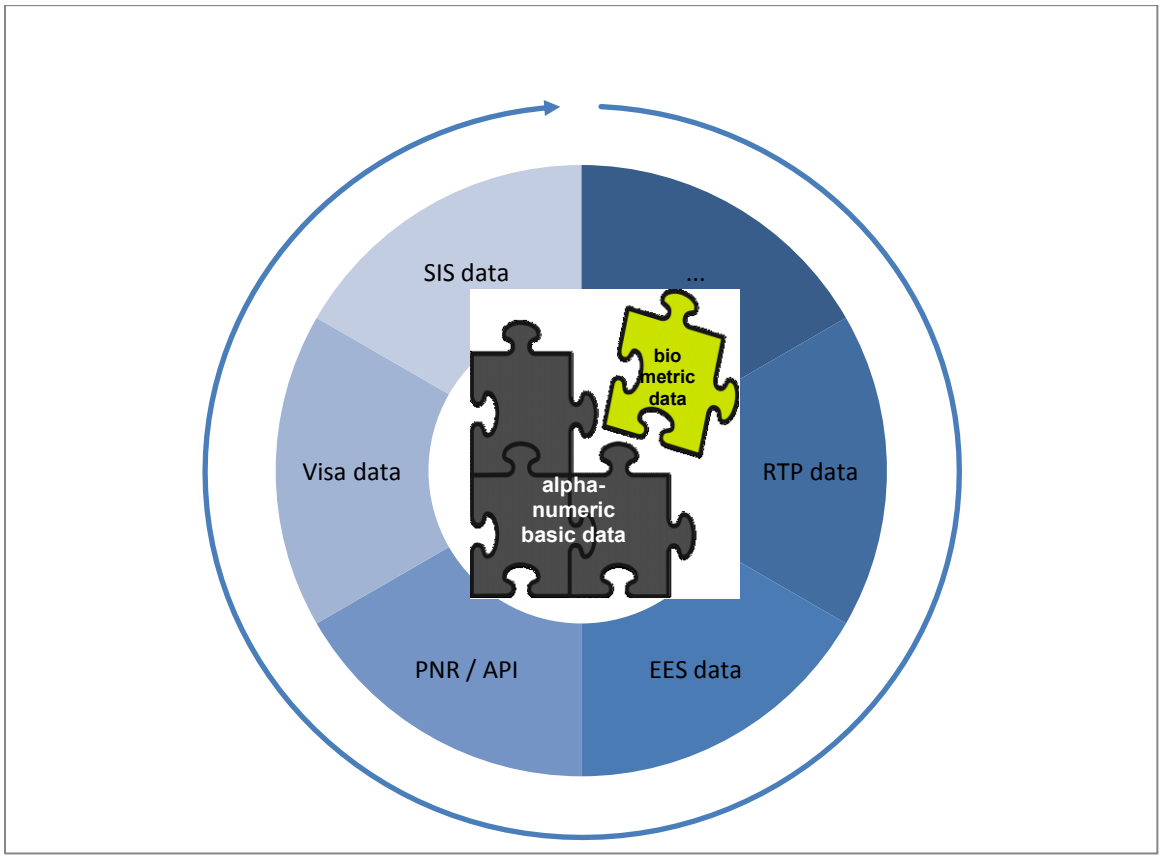

Figure 1: Objective of the approach

2. Advantages

"Once Only"

- Single collection and multiple use
- Data minimization
- Avoidance of redundancies and quality improvement
- Optimized processes for authorities and bona fide travellers, swift implementation, lower costs

Information networks

- Combination of information that has previously been stored separately
- Creation of an overall picture on the basis of the information available in the fields of travel, migration and security
- Security authorities are enabled to fully grasp the situation even in times of dynamic migration movements

Flexibility

- Easy further development by adding or removing individual elements
- Resource-efficient development, cost-effective operation of processes
- Easier way of finding compromises, extended political room for action

3. Need for action

It is necessary to reflect on these issues with a view to developing [in the long run] a modular and integrated identity management for travel, migration and security that combines the previous systems. From a legal, operational and technical perspective, this project is complex and will have to be gradually applied to existing and newly introduced systems. It must be examined whether the desired degree of information-sharing requires the centralization of decentralized systems (Prüm, PNR). All of these considerations should be guided by the desire to reduce unnecessary bureaucratic burdens for travellers and security authorities (once-only-principle). When it comes to implementation, state-of-the-art computational approaches (such as the universal messaging format UMF) must be taken into account.