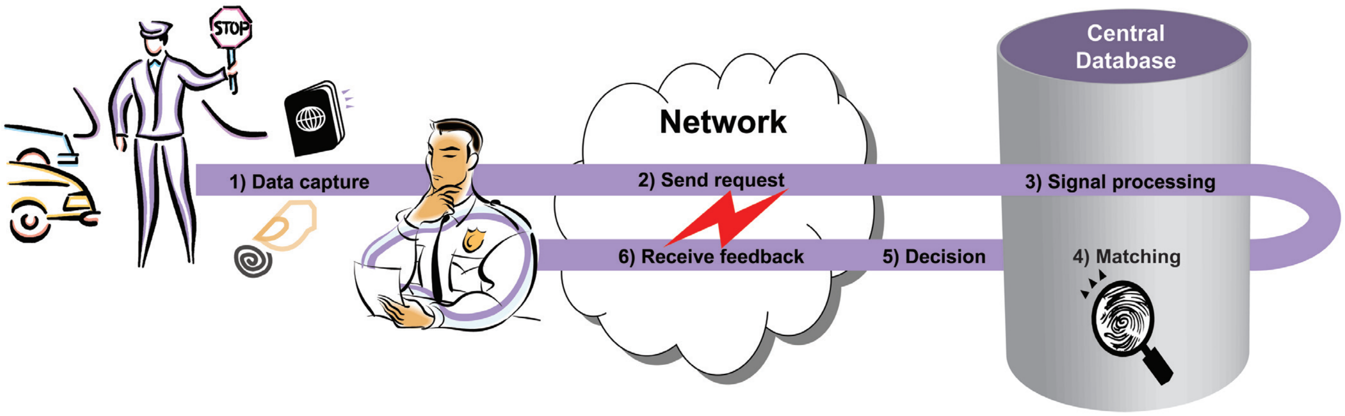
JRC Scientific and Technical Reports

Technical challenges for identification in mobile environments

Klaus Keus
Jan Löschner



EUR 24548 EN - 2010

EUROPEAN COMMISSION

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: Centro Comune di Ricerca
Via Enrico Fermi 2749, Ispra (VA) 21020 Italy

E-mail: Klaus.Keus@jrc.ec.europa.eu (National Detached Expert at the JRC)
Tel.: +39 0332 783073
Jan.Loeschner@jrc.ec.europa.eu
Tel.: +39 0332 785242

Fax: +39 0332 785469

http://www.jrc.ec.europa.eu

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC60747

EUR 24548 EN
ISBN 978-92-79-17049-2
ISSN 1018-5593
doi:10.2788/26072

Luxembourg: Publications Office of the European Union

Printed in Italy

Table of Contents

1. Executive Summary

In the same manner as the request for flexibility and mobility of people is growing, there is the need for adequate technology and processes to ensure the aligned convenience, security and protection of people and society. In subsequence to the mobility, new security scenarios arise, aligned by new challenges for technological, organizational and procedural contributions and solutions.

Keeping pace with mobility and technology trends while ensuring people's security, Mobile Identification will become a central goal. Devices has to be able to read and authenticate electronic identity enabling security documents[1] (see reference [1]) and to check electronically or digitally stored data - used for identification - against remote and complex national and international Information Systems. Looking for a common European wide security level, there is a strong need for harmonization of requirements and solutions. The result of an identification process should offer the same reliable results, wherever the process will be performed in Europe or in the Schengen Area. Common use of information for identification or exchange of identification results between the relevant agencies should become possible. These objectives require a whole bundle of tasks such as specifications for technology, for processes, for training and education and requirements for testing and standardisation.

This document describes some main technical challenges and requirements for identification of individuals in mobile (i.e. non-stationary) environments as e.g. required by the 'European Mobile Identification Interoperability Group (*MOBIDIG*)[2] [reference 1].

It is intended to support relevant stakeholders as law enforcement agencies or immigration offices, active in the area of identification of individuals in mobile environments. It offers some guidance for future technical work at the MOBIDIG to be respected in their work plan. Furthermore, it may be used as a first orientation for the general future work for identification in mobile environments using digital or electronically stored data.

After the introduction and some background of MOBIDIG and its policy context, the document presents the intention, main objectives and some information about the scope of work of the group. The following proposals, suggestions and recommendations presented are explicitly focusing on technology. Organizational and procedural issues are out of focus of this document and need to be addressed separately in further documents.

[1] **Remark:** Identification may be done by an electronic identity token: a physical device as an identity document or a hardware token or USB token

[2] E.g.: http://www.ants.interieur.gouv.fr/evenements/MOBIDIG-Presentation,161.html

The main part of the document is dealing with the technical challenges arising from identification of individuals in mobile environments. Some main architecture and their specific technical and organizational conditions are presented, distinguishing between local and remote solutions.

Requirements are defined and determined for selected technical issues. An intensified special focus is given to the main security issues. A proposal for related testing, evaluation and certification of devices is introduced, and security threats to be addressed for *identity token*, *devices*, for the *system* and in detail for communication and biometrics are presented.

Finally suggestions and proposals explaining how to deal with the technical challenges are presented in the way forward. User and application defined technical requirements have to be discussed with industry to give them the possibility to put the requirements into products and solutions which have to undergo a testing and evaluation. Early involvement of European Standardisation Organizations (*ESO*) will improve the chance to ensure of time-to-market standards. An open infrastructure as a middleware platform system offers the basis for testing including interoperability testing, simulating and demonstrating different scenarios, but also as a platform for further extensions, upcoming new technology and upgrades.

A future expansion of applications areas for mobile identification is encouraged. The use of identification of individuals for forensics in crisis management, for access control in mobile environments or for identification and tracking of goods, cargo or container via *RFID* in custom applications will enlarge the scope for possible scenarios and areas.

Preparing the technical platform and starting with the identification of individuals and the authenticity of identity token will open the door for future expansions for many security related application scenarios in mobile environment.

2. Rationale

Addressed in the political guidelines for the protection and security of the European citizens for the next ten years, related European wide harmonized collaboration in defending terrorism and crime, improving the security in the EU, protecting life and property and safeguard public order have become a central political concern. This is also expressed explicitly by numerous political programmes such as e.g. in the Stockholm Program[3] [2], in the related declaration of the European Council[4] [3] and in several recent press releases and announcements of the Commissioner for Home Affairs, Mrs. Cecilia Malstroem[5] [4]. Success in the prevention and combating of crime or any possible misuse in illegal immigration, detection and investigation of identity fraud depends on flexible and accurate identity checks, performed by law enforcement or

[3] http://www.sweden.gov.se/sb/d/11627/nocache/true/a/119953/dictionary/true

[4] www.consilium.**euro**pa.eu/uedocs/cmsUpload/st00006.en09.pdf

[5] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/987&format=HTML&aged=0&language=EN&guiLanguage=en

immigration agencies. New upcoming electronic identity technologies will support law enforcement and public safety enforcing organisations in forensics in crisis management after a disaster or of unconscious individuals after an accident. Future security technologies, embedded in the best organizational infrastructures and combined with appropriate secure procedures will deliver substantial contribution to become successful achieving the objectives. Common requirement needs, going along with a strong forcing need for harmonisation and technical interoperability will help to establish a required harmonized security level across borders for the whole EU and the Schengen area. This is the scope of work of MOBIDIG.

To reach these goals, there is a strong need to implement a platform which will help to define and determine technical, organizational and procedural requirements and criteria. It has to be enlarged by best practices and across-boundary exchange of information, of knowledge, of expertise and experiences between the partners and members. The work and results of related running activities and network should be respected.

This document will address upcoming technical needs and requirements for identification of individuals and the *authentication* in mobile environments using *electronic identity tokens* as required by the 'European Mobile Identification Interoperability Group (MOBIDIG)[6]. It should be understood as a discussion paper fostering the exchange of ideas and open for further enhancements and improvements to prepare the technical work of MOBIDIG. Additionally it should give some first general guidance for technology in the area of identification in mobile environments using electronic identity token for upcoming application areas.

It is based upon several presentations and discussions in the MOBIDIG and with representatives from national Police and Law Enforcement Agencies.

Even if there is wide range of aspects to be considered in the MOBIDIG work such as:

- technology and technical capabilities,
- functionalities and requirements of mobile devices,
- quality criteria,
- testing,
- electronic security and biometrics,
- related standards and protocols,
- information availability,
- data access and transmission,
- privacy and data protection,
- IT capacity and security,
- certification of equipments,
- data and users,

[6] E.g.: http://www.ants.interieur.gouv.fr/evenements/MOBIDIG-Presentation,161.html

- training and operational performance,

This document focuses on selected technical topics which are most relevant for further detailed consideration from the perspective of security, interoperability and testing.

3. *Introduction*

This document explains the background and offers some technical guidance for selected technical challenges linked to identification of individuals using identity tokens and the authentication of *ID documents*[7] in border control and law enforcement applications.

After a first introduction of the scope and the objectives of MOBIDIG in Chapter 4, Chapter 5 will introduce into the technical challenges, based upon the architecture selected. Chapter 6 will address in more detail some selected technical requirements such as the identity token, the data communication issue and the security. One main focus of Chapter 6 is going into detailed challenges in security such as testing and evaluation, security in token and devices, system security, and security related to biometrics and communication. Some guidance and recommendations for the way forward and an outlook for future extension will be given in Chapter 7. A summary and conclusion are given in Chapter 8. References and Acronyms, Abbreviations and definitions are covered by Chapter 9 and 10.

4. *MOBIDIG background / Policy context [8] [5]*

4.1. Relevance to current European Union context

As referred to in the Stockholm Program[9] [3], the internal security strategy to be developed in order to further improve security in the Union and thus protect European citizens against main risks and threats, should take into account “the challenges of the dynamic and globalised XXI century context”. High mobility, high speed communications and high speed evolution of technology, namely regarding travel and identity documents, are some of these challenges, offering new opportunities either to people who want to commit crimes, illegal immigration or to people who want to prevent and fight against crime.

Mobile Identification by means of handheld devices able to read and authenticate electronic and biometric security documents as well as to check against remote and complex national and international Information Systems is currently a precondition for keeping pace with mobility and technology trends while ensuring people's security. There are a variety of legal and constitutional approaches within Member States of the EU but in general police services in individual Member States aim to prevent and detect crime, protect life and property and safeguard public order.

[7] For details of ID token / documents look at Chapter 4.1.
[8] [1] 20100416 MOBIDIG short presentation POLICE COOPERATION WG
[9] http://www.sweden.gov.se/sb/d/11627/nocache/true/a/119953/dictionary/true

Immigration services aim to apply immigration controls effectively and to process applications such as visa requests. People, who are entering the country and/or the EU Schengen area, have to be checked to ensure that they are eligible. People who are not, have to be stopped, and - if necessary - to be removed.

Successful prevention, detection and investigation of crime are more and more depending on flexible and accurate Identity checks to be performed by law enforcement whenever and wherever necessary. In fact, the possibility of detecting identity fraud and of detecting and arresting criminals increases and thus public protection increases too.

Besides increasing efficiency and flexibility of law enforcement action and cooperation at national level, mobile identification is also crucial to build up a coherent and comprehensive approach towards an EU internal security strategy. This strategy necessarily includes the awareness of the links between local and organised crime, the prevention of cross-border crime and the implementation of the principle of availability. So, to have the right information to be available and/or shared at the right time, for the right person, and in the right place, upgrading and mobilising the necessary technological tools for the job and the adequate interoperable solutions and standards are urgently required.

Although these services can be distinguished from each other there are also many similarities, including the need to establish with confidence the identity of people they come into contact with, and the need to operate remotely, on foot, by car and sometimes on trains. There may in practice be overlap in operational work, for example when someone interviewed by immigration services at the border proves to be wanted by the police; or when someone spoken to by the police turns out to be an illegal immigrant. Cross-reference to the records of one service by the other can therefore be of considerable mutual assistance.

Working together to achieve these goals will contribute to “make operational cooperation more and more straightforward” as well as to cost and efficiency savings. Several ongoing national trials and projects or work under preparation in different EU-MSs or in the Schengen area demonstrate and underline the urgency and importance for harmonization and co-ordination. (see [6], [7], [8])

So MOBIDIG aims to give an adequate and appropriate response to mobility and flexibility needs and challenges in order to protect EU citizens in a global society.

4.2. Intention, scope and general objectives

The intention behind MOBIDIG is to address and bridge border control and law enforcement’s needs and challenges when performing Identity checks in mobile environments (trains, buses, in the street, in joint operations, etc). Handheld devices are to be available, as well as to look for common European requirements, standards and performance criteria.

MOBIDIG is basically sub-structured in the four following working groups:

1. Strategy,
2. Best Practice,
3. Technical aspects,
4. Legal background.

Mobile devices have important potential as an enabling technology for policing and other mobile enforcement services such as immigration and customs, as well as for police cooperation. But technology is still evolving and maturing and will require adaptation to key emerging technical changes in order to avoid waste of national efforts and investments. So, collaboration and guidance at EU level aiming at reaching conclusions on the most cost-effective use of this technology and potentially to develop common solutions is highly relevant.

Mobile Identification and related mobile devices are currently a precondition for keeping pace with mobility trends while ensuring people's security. Successful prevention, detection and investigation of crime are more and more depending on flexible and accurate ID checks to be performed whenever and wherever necessary.

Making use of the relevant new technologies and the adequate interoperable standards and solutions is urgently required to ensure the “right information available at the right time, for the right person, and in the right place”.

Besides increasing efficiency and flexibility of law enforcement and immigration actions and related cooperation at national level, mobile identification is also crucial to build up a coherent and integrated approach towards an EU internal security strategy as foreseen in the Stockholm Program, which necessarily includes the implementation of the principle of availability of information.

The main operational scope of MOBIDIG is the identification and verification of people's identity by means of the authentication of identity enabling documents (non-electronic, electronic and biometric passports, ID cards, residence permits, driving licences, etc) and/or by checking against remote national and international databases and Information Systems.

Having this frame in mind, MOBIDIG will provide its members with a platform to present and debate their needs and experiences, to exchange updated information about ongoing work and national activities and to learn from each other. It will also be a relevant forum where to set up and agree upon a common and updated guidance to needs and challenges on mobile identification. This includes inter, alia, the lack of exchange of information and co-ordination between countries, agencies, industries and end-users, the lack of standards, the requirements for reading and/or capturing biometrics, for certification and testing as well as for communication to back-end systems.

Briefly, MOBIDIG is expected to promote the exchange of information and to give guidance towards EU harmonization and standardization, interoperability on mobile identification and mobile devices, paving the way for further cooperation and coordination.

Mobile technology has been developing quickly and has increasing potential to increase the speed and efficiency of police and immigration services in identifying people they come into contact with. There is a potential market of tens of thousands of devices across the EU.

In conclusion, the EU MOBIDIG group aims to raise awareness of mobile controls and ID checks and to promote best practice and effective use of the technology, where this would increase the efficiency and cost effectiveness of police and immigration services.

5. The Architecture

5.1. General Architecture

MOBIDIG is working to assure that systems, equipments and components used in a European wide harmonized way will meet at least the following two **basic objectives**:

1. **secure and reliable identification of persons** (*Identification* (1:n) and *verification* (1:1) of people's identity[10]),
2. **secure and reliable authentication of the identity token used** (e.g. Authenticity of identity enabling documents),

where the **relevant data** to be respected for these processes may be:

1. held **in identity enabling documents**, or
2. stored **in local and/ or remote** databases.

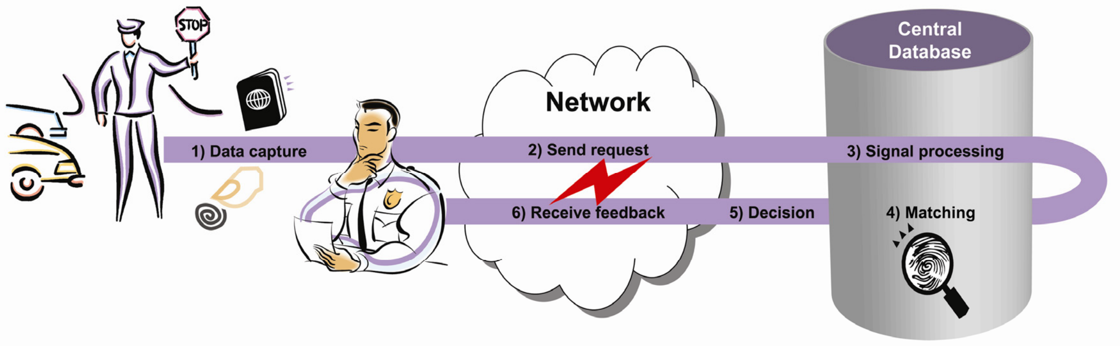


Figure 1: Illustration of an architecture where the relevant data is stored in a remote database, separated in the different main phases

According to [9], there exist 4 general **application architectures:**

1. **Remote** (1:1 or 1:n) or
2. **Local** (1:1 or 1: n).

Thus the different application architectures have to be distinguished into two different main approaches (see Figure 2):

[10] Identification (1:n): to look for the persons identify in a list of possibilities (e.g. black list) ,
Verification (1:1): to check if the person is identical with the person it claims to be

1. Standalone **Local System**[11] (= 'all-in-one device' or 'system') or a set of several components (e.g. sensors) or devices composed to one system (case (a)), and
2. local devices, connected to a central system (**Remote (Distributed) System** (cases (b) – (d)).

The different approaches may differ in technical and/or organizational requirements. The 'remote distributed approach' may be sub-divided into three further architectures (b) - (d). Each of them is based upon specific technical features and framework conditions.

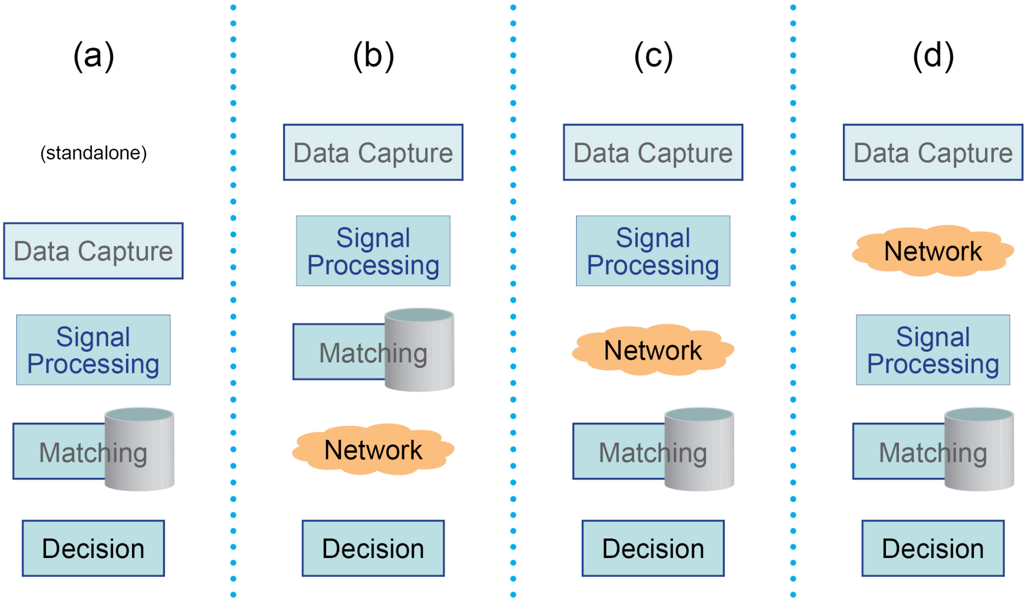


Figure 2: The overall architecture and the main phases [12] [9]

5.2. The detailed Architecture

As expressed in Figure 2 each application process is subdivided in the five main **phases**:

1. Data capture,
2. Signal processing,
3. Matching,
4. Decision, and
5. Communication.

As the first four phases are dealing with the identification, verification or authentication itself, the communication phase is responsible to transfer the data from local station to the remote central station and backwards or even on local level between the different devices or sensors. This has to be done in a secure and reliable way (for details look at Chapter 6.3). The local communication may be wired or wireless, depending upon the application and scenario requirements and the

[11] Meant in the sense of 'the interaction between people, algorithmic processes, data and technology'

[12] Source: NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0, S. Orandi / R. M. McCabe, NIST, Information Access Division, Information Technology Laboratory, 08/ 2009

environment. Communication from local to remote (= central) and backwards most times will be performed using a wireless connection.

So the overall architecture may be split into two core *task areas*[13] (1) – (4) and (5):

1. the **identification and authentication** process (local or remote part of) and
2. the **communication** process.

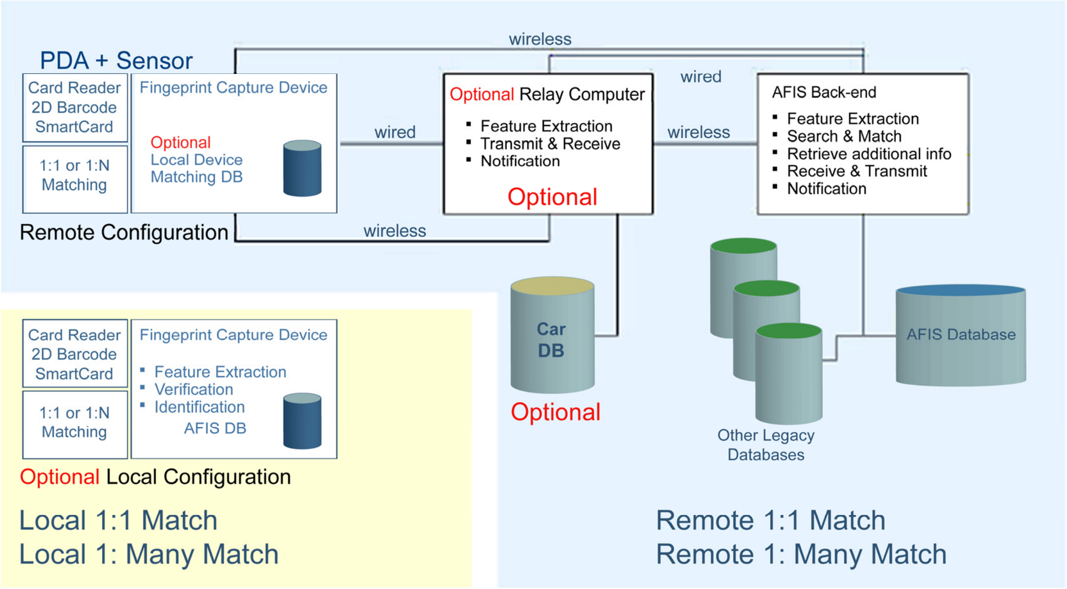


Figure 3: The detailed architecture and related communication infrastructures [14] [9]

5.3. An Application related Architecture Structure

The presented architecture will be able to represent a number of MOBIDIG *application scenarios*. The top level scenario is as the acronym says ‘mobile identity’, split into the *scenarios* for law enforcement and for immigration control. Application scenarios could be:

- border control,
- on the street person verification,
- on the street Identity Document (ID) authentication,
- person identification, or
- car verification, etc.

These application scenarios can be subdivided into *application areas*. For border control for example this could be the different areas a border control post (*BCP*) could work such as a road crossing, a pedestrian crossing or railway border etc. The application areas could be seen as a

[13] **Remark:** ‘*Task area*’ is meant as a single or a set of combined phases (1) – (5)

[14] Source: NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0, S. Orandi / R. M. McCabe, NIST, Information Access Division, Information Technology Laboratory, 08/ 2009 [9]

combination of different *use cases*. Taken the railway BCP example, possible uses cases could be:

- regional train,
- high speed connection,
- EuroStar, etc.

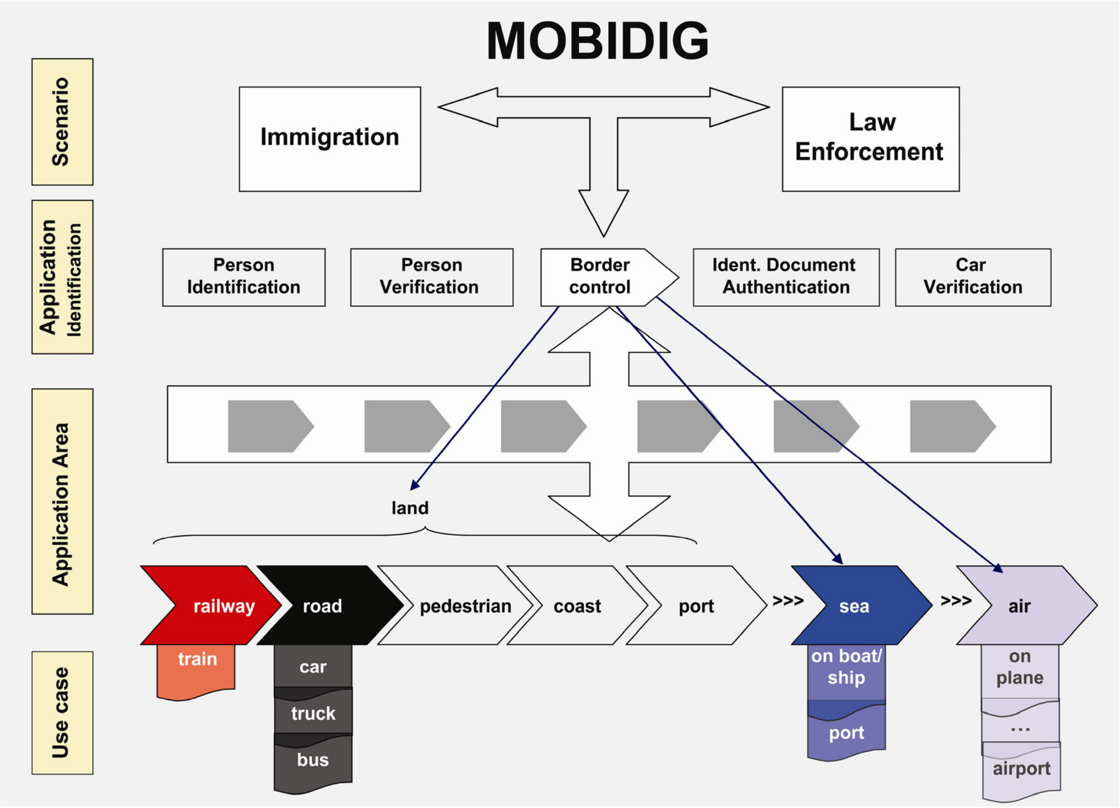


Figure 4: Application related Architecture Structure (AAS)

Following this proposal the MOBIDIG scenario would consist of a number of application scenarios, which themselves would consist of a number of application areas and this would be subdivided into a number of use cases. This proposal and the associated terminology are necessary to establish a common understanding and associated vocabulary. In a next step MOBIDIG could prepare lists of realistic and practical application scenarios, application areas and use cases. Once this list is prepared and available, MOBIDIG could prioritize the elements on the list for each category. At the end each element could be associated with technical requirements such as described in the next chapter.

In [9] ten different scenarios for Mobile ID devices have been defined alternatively based on risk levels to public safety and also on the intended function. A number of mobile identification use cases applicable to fingerprints, face, and iris are define. It is for example not taking European specifics like the implementation of EAC in passports into account.

6. Some Technical Requirements

The basic technical requirements are defined by a number of ISO standards, national norms, the national and international legal systems and technical reports.
All the objectives addressed in Chapter 6 encompass a wide range of aspects, as technology and technical capabilities, functionalities and requirements of mobile devices, electronic security and biometrics, information availability, data access and transmission, privacy and data protection, *ICT* capacity and security, related standards and protocols, quality criteria and testing, certification of equipments, data and users, training and operational performance.

Based upon the distinctions in the architecture made in Chapter 5 there exists a large set of technical requirements to be addressed such as for (not restricted to):

- Reader (e.g. *MRZ,* Chip, barcode, …),
- Conformity, testing (including compliance and interoperability) and certification of reader and devices,
- Capturing device requirements (biometrics (e.g. fingerprint, iris, face, ...),
- Biometrics interchange requirements, matching SW, quality control, compression,
- Computing platform and human interface,
- Communication platforms / protocols incl. *MESH*,
- Additional special requirements for communication (e.g. *GPS*)
- Security and Privacy issues (data resident on the device or central storage),
- Security of the communication (incl. confidentiality, integrity, availability, robustness, backup / recovery and continuity, user authentication, device authentication, *EAC*, *BAC*, login / audit trail, …),
- Testing and certification of system,
- Usability and environmental needs,
- Ergonomic issues,
- Charges, battery,
- …

As mobile ID device can be used in a variety of different contexts, of which the following are listed in [9]:

- such as a law court
- airport terminal,

- by a patrol officer on the street or in a patrol car,

These different use cases require as well different levels of resistance to environmental factors such as temperature, humidity, dust, water, vibration, etc. For these reasons [9] develops three different profiles (Indoor, Law Enforcement and Military), with increasing levels of resistance to the relevant environmental conditions.

In the further ongoing, this chapter will focus on selected technical topics which are most relevant for further detailed consideration.

6.1. Identity Token

Conform and trustworthy identity token are prerequisites to achieve the objectives mentioned in Chapter 3.1.

Possible tokens to be considered to perform a secure and reliable identification and envisaged to be used and taken into consideration could be e.g.:

1. *BAC* / *EA*C EU e-passports,
2. BAC non EU e-passports,
3. National e-ID cards,
4. e-Residence permit,
5. Credit cards,
6. E-health care card, or
7. Driving and e-driving license.

Authenticity and authentication of the token require physical features checking and / or remote connection to a ‘database’ to check the status of the document.

6.2. Data communication issues

Data communication may be wired or wireless. Different application scenarios, related environment conditions and the availability of needed communication infrastructures require and lead to different technical solutions. Even if there are running first national trials, a lot of open issues and challenges need to be solved. The current national trials are based majorly on available commercial private communication infrastructures. Commercial networks, including *3G* or forthcoming *4G* networks as used for mobile phone networks, may be probably a cheaper and currently available option. Connectivity can become an issue. But what is about security or availability? Emergency services networks based on *TETRA* (including *Tetrapol*) standard as a highly resilient network for use by emergency services will be much more appropriate because of security and availability reasons, but first national implementations and trials are very limited, cross-border trials are very restricted. These specified public communication infrastructures might be desirable, but likely they will lead to higher costs than a conventional commercial solution and

may offer less bandwidth (speed of data transmission) than *3G* and certainly *4G* connection. Others solutions may be integrated with professional mobile radio (*PMR*) network. If *Bluetooth* for 'nearby area' or *NFC* for 'near field communication' will be selected: What about performance and security?
The area of data communication is still an open issue and needs much more focus in the next future.

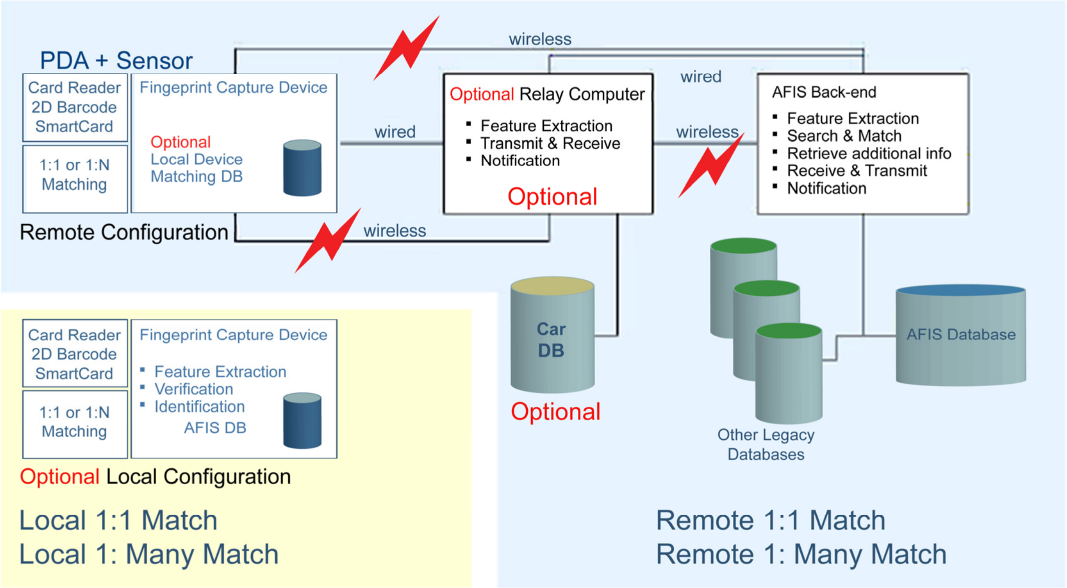


Figure 5: The most critical parts of communication in the communication infrastructures[15]

The communication is not restricted to the connection from a local to a remote station, i.e. handset and communication network connected to (remote central) core systems or the handling of incoming communications from mobile devices into the central network including the handling and managing of security issues, firewalls, or authentication requests (Figure 5).

On local level (for details see Figure 6), additional communication issues have to deal with the local connection of components to a mobile local system, e.g. a device connected to a single integrated unit. This might be a master unit, a keyboard, a screen, a communication module, a biometrics reader (e.g. fingerprint reader or a camera for face recognition) or a token / document reader. All these components may be separated, connected to one system. So the technical question will raise how to connect on local level.

[15] Source: NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0, S. Orandi / R. M. McCabe, NIST, Information Access Division, Information Technology Laboratory, 08/ 2009

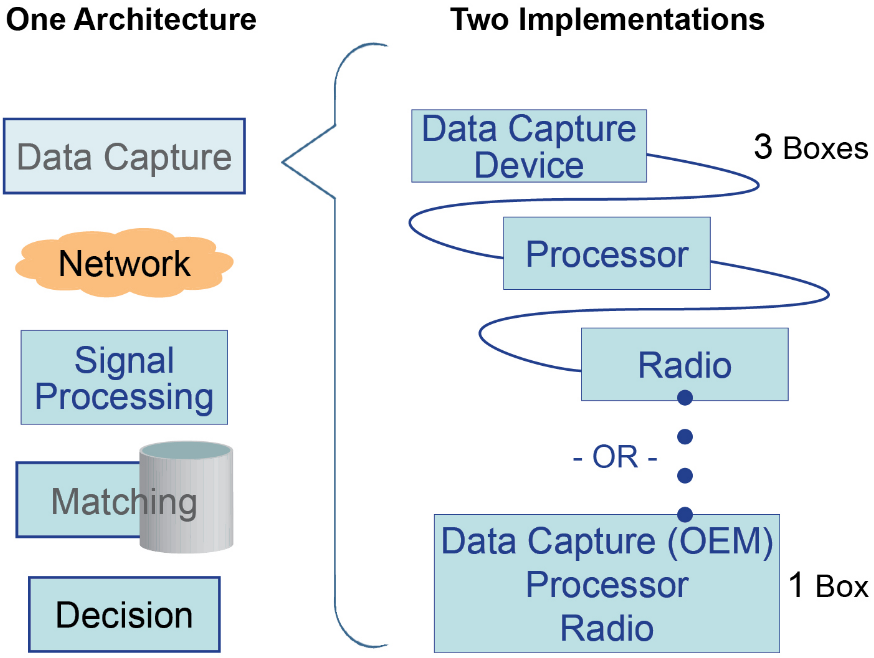


Figure 6: The stand-alone local systems and related possible implementations [16]

6.3. Security Issues

Security is the most crucial and critical issue for the applications foreseen by MOBIDIG. It is vital that the final decision is done upon reliable information and not misled by any compromised (interim) step. Based upon a scenario defined security and risk model, particular risks need to be analyzed and managed, values (HW, SW, data, information) need to be protected against any kind of threats, from technical via organizational to procedural ones. Specific use cases and application cases oriented security models including related risk management are core substantial element in the security perspective of the MOBIDIG work including ethical questions - e.g. dealing with privacy. But these issues are outside of the scope of this document. Use case based security models might be defined based upon Security or Protection Profiles (*PP*) (see Chapter 6.3.1).

In conclusion, numerous possible security threats in a mobile application environment shall be respected under the umbrella of MOBIDIG. However this document will concentrate on those selected areas addressed in the following six security elements: In sub-chapter 4.3.1 it will start with a short introduction to the existing *Common Criteria* (CC) Scheme for testing, evaluation and certification, followed by the sub-chapters 6.3.2 – 6.3.6 which offer an introduction into

[16] Source: NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0, S. Orandi / R. M. McCabe, NIST, Information Access Division, Information Technology Laboratory, 08/ 2009

- Security in token,
- Security issues in devices,
- System security,
- Security issues in biometrics, and
- Security issues in communication.

6.3.1. Existing Testing, Evaluation and Certification Scheme: the CC-Scheme

Where applicable the Common Criteria for Information Technology Security Evaluation could be applied to assess the security issues. Applied to MOBIDIG, the existing Common Criteria Certification Scheme could become a framework in which end-users specify their security functional and assurance requirements (e.g. using the Protection Profile (PP) approach) to express their needs. These PPs might be used as a pre-definition for vendors for the development and implementation of products and to claim its security attributes. Evaluation Bodies (evaluation facilities / testing facilities / laboratories) evaluate the products validating the user's requirements against the vendor's claims and certification bodies issue a certificate if the evaluation was successful. In this sense Common Criteria certification applied to the MOBIDIG domain and its use cases provides assurance that the process of specification, implementation and evaluation of devices and components has been conducted in a rigorous and standard manner.

How complex dependencies could be in the MOBIDIG environments is illustrated in Figure 7.

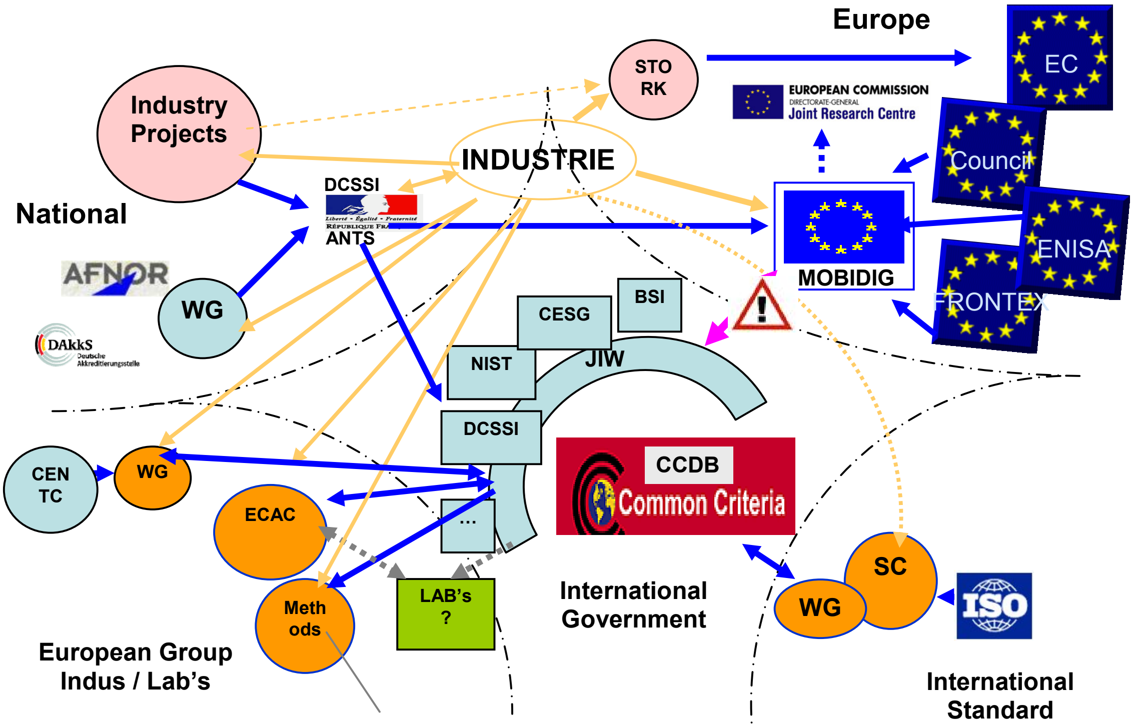


Figure 7: Complex CC dependencies

The Common Criteria for Information Technology Security Evaluation (CC)[17] [10] and the companion Common Methodology for Information Technology Security Evaluation (*CEM*) are the technical basis for an international agreement, the 'Common Criteria Recognition Agreement (*CCRA*)', which ensures that certificates issued by a member of this agreement will be recognized by all the other CC-agreement members, based upon a mutual recognition agreement.

In general, the vendor declares a so-called Security Target (*ST*) which defines the security objectives for his specific product, related security functions and the strength of implemented security ensuring functions (technical mechanisms) defining the level of assurance which will become the basis for the foreseen evaluation. So the product will be evaluated against the vendor's specified security claims. The evaluation of the product itself against the ST will be performed by competent and independent accredited evaluation bodies so as to determine the fulfilment of particular security properties in the ST to a certain extent or assurance. [10]

Supporting guidance is used within the Common Criteria evaluation and certification process to define how the security evaluation criteria and related evaluation methods are applied. MOBIDIG should prepare a list of relevant technology use and most appropriate use cases (see Chapter 5.2) including security requirements for all the elements in the architecture.

[17] (http://www.commoncriteriaportal.org/thecc.html)

The certificate of the security properties of an evaluated product can be issued by Certification Bodies as part of the Certification Schemes, based on the result of the evaluation by the Evaluation Body. As in ICT security, the CC can become the driving force for the widest available mutual recognition of mobile identification systems.

6.3.2 The Protection Profile Approach

As an enhancement to the specific product oriented, proprietary vendor defined ST, there exist a more general and generic approach which is used defining a whole set of security products and components. So-called Protection Profiles (*PP*) (see [12]), independent from the vendor specifications - is typically created by a user or user community, in our case this could be MOBIDIG - and provide a specific product independent specification of information assurance security requirements. A PP is a combination of threats, security objectives, security assumptions, security functional requirements (*SFR*s), security assurance requirements (SAR) and a rationale. A PP specifies generic security objectives evaluation criteria to substantiate vendors' claims of a given family of information system products. Among others, it typically specifies the Evaluation Assurance Level (*EAL*), a number 1 through 7, indicating the depth and rigor of the security evaluation, usually in the form of supporting documentation and testing, that a product meets the security requirements specified in the PP.

It is suggested that MOBIDIG should collect existing PPs of all components used in mobile systems as described in [13] and complement them with PPs not available or foster the development of such PPs and promote a harmonized *CEM*.

6.3.3. Security Issues in Identity Token

The final result and decision of the identification, verification or authentication process strongly depends on the reliability of the token, i.e. the physical device storing data to be used to perform the identification. In the applications focused in this document and as introduced in Chapter 6.1, the identity token may be an electronic ID document such as an ePassport, a national e-ID card, a credit card, an e-driving license or similar. The data used for identification or authentication purposes often is stored in digital or electronic form in an embedded chip.

The system shall check at least for possible physical threats such like

- Faked or forged token,
- Forged identity,
- Incomplete or inappropriate identity data,
- Destroyed physical data in token,
- Destroyed data storage (chip) or its physical access.

Organizational threats such like

- Theft or loss of token, and
- Expiration of token may be checked against central stored information.

Further threats are dealing with the digital data stored in the identity token, as e.g. destroyed or modified data stored in the chip, modification or faked signature of the issuing authority. Most of the checks for physical threats may be done locally by security functions in the device. Some checks need access to central stored information e.g. the check for lost or theft, but also the verification of the signature of the data stored in the chip.

6.3.4 Security Issues in Devices

It is vital that mobile devices may not be used to compromise the security of connected systems (HW and SW), data and information. As explained in the previous chapter, security threats for devices may also be subdivided in technical, organizational and procedural ones. ICT related threats may be addressed by classical ICT security countermeasures and will not be explained in further detail in this document.

Particular risks that need to be protected against include at least:

- Overlooking devices while they are in use by authorised users,
- Unauthorised access to a mobile device,
- Interception of communications with the mobile device, including passive listening and recording,
- Cloning or replication of a valid device, including authentication and access codes,
- Wireless compromise of mobile devices,
- Vulnerability of mobile devices,
- Theft / loss of mobile devices,
- Attacks against core systems via the device.

Threats such like theft, loss or cloning of mobile devices may be covered by organizational procedures (e.g. using an appropriate management of devices) which may be supported by technical countermeasures such as tracking of devices or remote authentication mechanisms. Classic ICT security countermeasures such like firewalls including device authentication mechanisms will help to cover the problem of attacks against the core system. User identification and authentication will avoid unauthorized access to the device. Adequate and state-of-the-art implemented anti-virus SW will help against possible SW attacks via wireless communication. Device authentication mechanisms (e.g. as EAC) will ensure that only registered devises (as e.g. the readers devices) will have access to the documents. Approved tempest testing combined e.g. with EAC will help against passive listening or eave dropping of information.

6.3.5. System Security

The security system describes and relates to all elements proposed in the MOBIDIG architecture (see Chapter 5.1) in regard to its security. Basically it is the collection of existing PPs for sub elements of a MOBIDIG system and the discussion of the feasibility to define a MOBIDIG system PP. At the stage of designing and accessing the MOBIDIG system tools like P3P, OCTAVE or CRAMM, which were used in the past at the JRC, can help to tailor the system security to the needs.

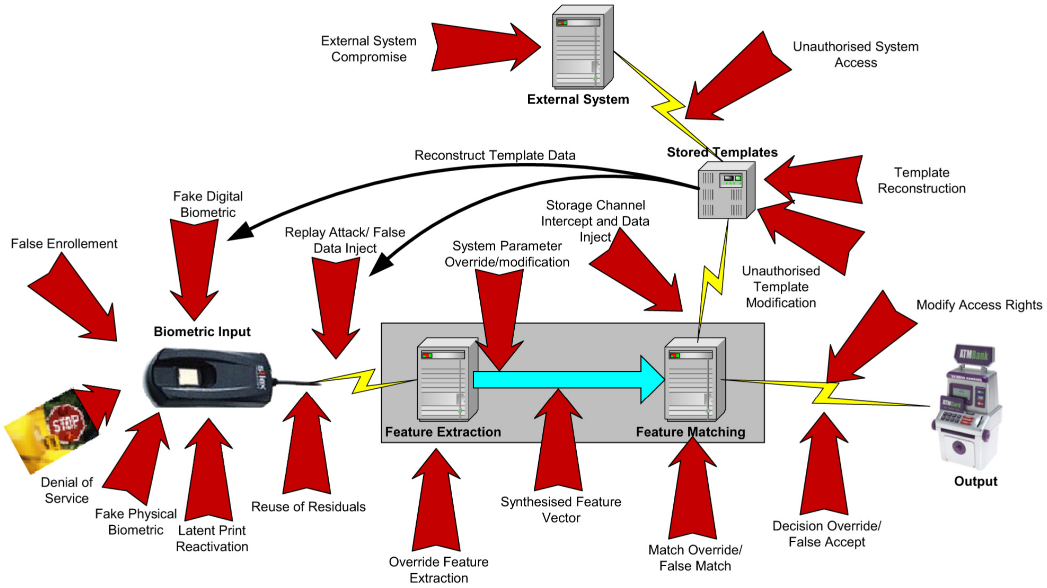

External System Compromise
External System
Unauthorised System Access
Reconstruct Template Data
Stored Templates
Template Reconstruction
Fake Digital Biometric
Storage Channel Intercept and Data Inject
Replay Attack/ False Data Inject
System Parameter Override/modification
False Enrollement
Unauthorised Template Modification
Modify Access Rights
Biometric Input
Feature Extraction
Feature Matching
Output
Denial of Service
Fake Physical Biometric
Latent Print Reactivation
Reuse of Residuals
Synthesised Feature Vector
Override Feature Extraction
Match Override/ False Match
Decision Override/ False Accept

Figure 8: Security threats related in the 'Remote Distributed System[18] [11]

6.3.6. Security Issues in Biometrics in mobile Applications

As biometrics is increasingly being used for security related identification and authentication purposes, it has generated considerable interest from many parts of the information technology security community. Of course, as biometrics is still a relatively fresh technology, originally never foreseen for real security contributions, in the meantime it is used more and more in secure applications and is enhancing security in specific applications too. This implies, that there is a large deal of interest from those interested in examining and researching methods of circumventing and compromising biometric systems, and in contradiction of course from those developing adequate new countermeasures for protection.

[18] Source: Biometric attack vectors and defenses, C. Roberts, in 'Computers & Security (2007): www.sciencedirect.com

In common with all security systems, there have been attempts to circumvent biometric security since they were introduced, partly solved in the meantime, partly still not solved or under research or development.

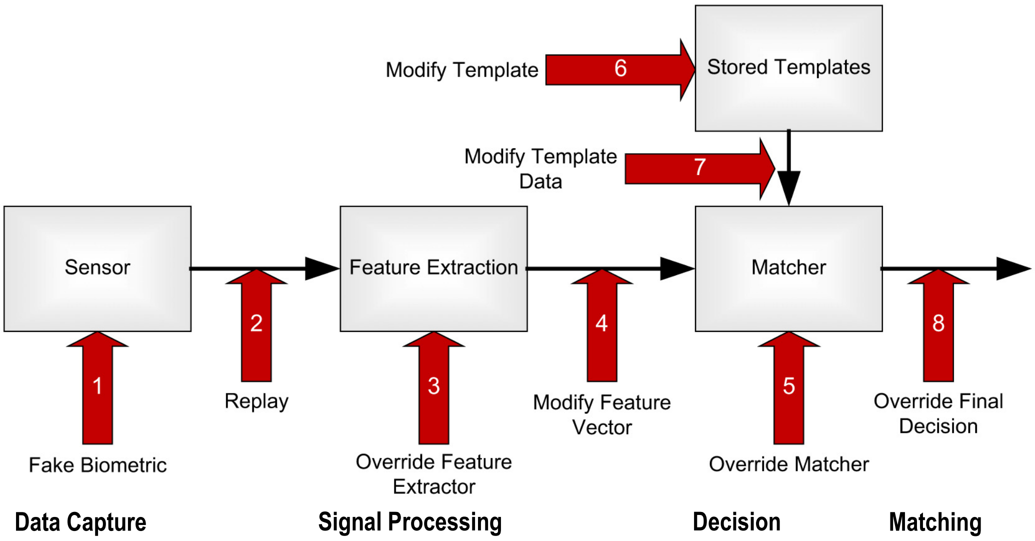


Figure 9: Security threats and attacks in Biometrics Systems [19] [11]

The vulnerabilities 1-8 are common to many ICT Systems, partly enlarged or adopted with security specific enhancements for biometrics (e.g. the feature specific sensor SW, compression algorithms, specific requirements to ensure the privacy and possible misuse of biometrics (e.g. biometrics keys), requirements for spoofing etc:

- operating systems (server, workstation);
- storage management systems (operating system, application);
- biometric applications;
- sensor software;
- Hardware / firmware.

Other key aspects include:

- operations management;
- remote management (particularly of *FAR*/*FRR* parameters);
- system configuration.

The following Table 1 gives an overview of possible treats in biometrics and possible countermeasures.

[19] Source: Biometric attack vectors and defenses, C. Roberts, in 'Computers & Security (2007): www.sciencedirect.com

Threats / Countermeasures	Input device protection	Input data protection	System data protection	Data Storage	System tamper resistance	Secure communications
Challenge/response	✓	✓	✓	✓	✓	✓
Randomising input		✓	✓		✓	
biometric data						
Retention of data		✓	✓		✓	
Liveness detection		✓	✓		✓	
Use of multiple biometrics		✓	✓		✓	
Use of multi-modal biometrics		✓	✓		✓	
Use of multi-factor authentication		✓	✓		✓	
Use of "soft" biometrics			✓		✓	
Signal and data integrity and identity		✓	✓	✓	✓	✓
Encryption and digital signatures		✓	✓	✓	✓	✓
Template integrity			✓	✓	✓	
Cancellable biometrics			✓	✓	✓	
Hardware integrity	✓	✓	✓	✓	✓	
Network hygiene	✓	✓	✓	✓	✓	✓
Physical security	✓	✓	✓	✓	✓	✓
Activity logging, policy & compliance checking	✓	✓	✓	✓	✓	✓

Table 1: Defence measures in biometrics[20] [11]

6.3.7. Communication Security

As introduced in Chapter 6.2, data communication and related security issues are central elements for a secure and reliable exchange of information, on local and on remote level. Most of the challenges and related risks and threats are well known and independent from the special application scenarios addressed by MOBIDIG, a lot of them are solved or related countermeasures are under development or part of recent research.

In special for the mobile application scenarios the main new challenge is to transfer those solutions to the specific communication infrastructures which will be selected and applied in the concrete situations and applications for mobile identification, verification and authentication purposes. Because there don't exist sufficient experiences so far, the use cases have to be

[20] Source: Biometric attack vectors and defenses, C. Roberts, in 'Computers & Security (2007): www.sciencedirect.com

defined, related risks have to be analyzed, evaluated and prepared for managing. Related countermeasures have to be verified, implemented and validated under these specific conditions.

Main risks are dealing e.g. with the interception of communications with the mobile device, including passive listening and recording (eavesdropping) and also unauthorised users being able to introduce their own transactions to access information (e.g. so-called man-in-the middle-attack). Even if information transmitted or held on a mobile device cannot be compromised, the use of mobile devices by the police or other enforcement agencies may be detectable and may give away the possibility of future or imminent operations; or may allow the use of such devices to be blocked or disrupted (e.g. by interferences attacks).

A further central communication security risk is the wireless compromise of mobile devices. The existence of a wireless (e.g. radio) connection to a mobile device may allow a hostile attack in which software on the device is altered or replaced by a malicious third party, possibly without the user or operator being aware of any change.

Classical security countermeasures may have to be adopted and applied (maybe it needs to be tailored for the specific purpose of MOBIDIG) such as encryption, the use of *VPN*s (Virtual private Networks) or remote operation and maintenance including e.g. deletion or blocking of commands. Encryption is used to ensure the confidentiality of communications. Virtual Private Network (VPN) provides a secure end-to-end connection with authentication and integrity ensuring mechanisms. Remote operation commands may be used to change or modify instructing a mobile device that has been lost or stolen to delete any sensitive data including access codes or authorizations that it is holding. Additional countermeasures should help to ensure the permanent availability and support robustness and resilience against possible Denial of Service attacks (*DoS)* or interferences attacks. Architectures shall respect backup lines or recovery solutions to ensure the continuity which may become critical e.g. in a critical incident case such like a disaster.

The handling of incoming communications from mobile devices into the central network and the related security management (e.g. managing the firewalls, authentication, etc.) has to be considered. Communications and security issues in local networking of components building a mobile solution have to respect devices connected to a single integrated unit (master unit, keyboard, screen, and communications module; e.g. fingerprint reader and/or document reader). Connecting different separated components or sensors building a *MESH* has to be foreseen. Depending on the case and the technology of the connection link (including the selected protocol) additional security solutions have to be defined.

7. Recommendations and possible way forward

As the area of identification of individuals using electronic identity token in mobile environment is a very new challenging area, there does not exist any available guidance or best practices how to deal with it. It is a very complex area, even if often same or similar technology and technical devices are used, accessing and using the same data across different application areas. It is addressing a large variety of applications scenarios within a huge set of different framework conditions. So an innovative and more constructive approach – e.g. based upon a layered structure - is necessary to prepare the upcoming work.

To ensure a better flexibility for future use cases, the technical requirements set of MOBIDIG may be built using the 'Application related Architecture Structure' as introduced in Chapter 5. Before starting to define the concrete detailed technical requirements, it would be helpful to have a structured overview of different levels as application scenarios, application areas and use cases. Application areas should be defined to determine the focus such as BCP for pedestrian, at the coast or in ports, in trains or buses or at airports. Results of running or finished projects such as *EFFISEC* may be respected to look for synergies. Use cases e.g. are mobile verifications of the identity persons at any BCP, based e.g. on e-passports, or any other relevant electronic identity document foreseen in the future spectrum of tokens. Conformity and security issues of the documents and the IS used should be analyzed. Projects such as EuroStar might become one of the interesting use cases.

There is a need for use cases and related profiles which will help to define and specify more specific tests such as testing of Biometric performance under different environmental conditions, or IS performance with different passport personalization. Each use case may have specific security requirements and may require an individual security level. All these elements have to be are respected in the security policy and the security concept.

Another important area to care about is the identity token itself. A conform token is a prerequisite to achieve the objectives defined in Chapter 6. It would be helpful to prepare a list of tokens envisaged to be used and taken into consideration. Based on this list a specific overview of the token authentication mechanisms to achieve the authenticity has to be created. Based on the list of authentication mechanisms a list of the prerequisites can be established. In case of the example of e-passports the prerequisite is to have a *CSCA* certificate from a trusted source. In this specific case MOBIDIG should be made aware of an EC attempt to coordinate a joint membership of the EU member states to the *ICAO PKD*. For testing purposes it is necessary to get a set of relevant token from MSs. Industry should be encouraged to contribute the devices to be used during the test procedures.

Testing objectives and related testing procedures and methodologies have to be determined. Besides the classical ICT security objectives such as confidentiality, integrity and availability additional issues have to be respected such as:

- interoperability and performance (e.g. in biometrics, in communication or system performance),
- robustness as spoof resistance in biometrics,
- the resistance of communication against interferences,

- data transfer for biometrics identification against black lists,
- related bandwidth used for communication and
- privacy issues in biometrics (template protection) or communication (encryption).

In respect to the introduced structure above, the needs and requirements contributed by the user communities have to be collected and a first structured set of technical requirements has to be created.

It is strongly recommended to use existing knowledge, expertise and experiences from different trials and projects in these areas.

Existing testing labs and infrastructures related to identification purposes - such as successfully installed and operated by JRC - should become heavily involved using the deep experiences and facilities for testing of interoperability in ePassports. Existing expertise in biometrics including running projects such as the *BEST NETWORK*[21] [15], existing deep knowledge in secure communication for safety and security (e.g. in *TETRA / TETRAPOL*, in 3G and 4G for communication, or further special knowledge for wireless communication) e.g. in JRC or in the *FORERUNNER*[22] [16] project are important contributions.

Besides the concrete user and application defined technical requirements to deal with, a lot of other topics need to be addressed. First of all, there is a strong and urgent need to discuss technical requirements with all relevant stakeholders, in special with industry as early as possible. This would give them the possibility to put the requirements into products and solutions which have to undergo a testing and evaluation. Early involvement of European Standardisation Organizations (ESO) will ensure the availability of time-to-market standards and the chance to define related harmonized testing methodologies.

It would be useful to define a first possible use case as part of an application area to be used for demonstration purposes. Implemented in a demonstrator, it may be used as a nucleus for expansions for further use cases and combined for an application area. The implementations may be used to analyze and examine related consequences and impacts. Finally it may be expanded for testing, and to be used as an experimental system and for simulation.

An open infrastructure as a middleware platform system offers the basis for different perspectives of testing including interoperability, for simulating and demonstrating different scenarios, but also as a platform for further extensions or upcoming new technology or upgrades.

A future expansion of applications areas, application scenarios and scenarios for mobile identification should be encouraged and foreseen. The use of identification of individuals for

[21] Best Network: http://www.best-nw.eu/

[22] http://www.tetramou.com/uploadedFiles/Files/Documents/Column%20Verbinding%20januari%202010%20%28Europese%20ontwikelingen%20ISI%20+%20breedband%29.pdf

forensics in crisis management, for access control to areas or buildings in non stationary environments is based upon similar technology and processes. This technology may become applicable for identification and tracking of goods, cargo or container using e.g. RFID technology in custom applications enlarging the scope for possible application areas.

Preparing the technical platform and starting with the identification of individuals and the authentication of electronic identity token offer the chance for future expansions for many security related application scenarios and scenarios in non-stationary environment.

8. Conclusion

This document has led into the upcoming technical challenges for identification of individuals in mobile environments. Based upon the example and requirements of the MOBIDIG, focusing on the applications for law enforcement and immigration services, several models for possible architectures and its related technical challenges were presented. As these application areas and scenarios are very security sensitive, a major focus was given on security issues and it became obvious that related security and security testing are major concerns. Existing evaluation and certification schemes such as the CC scheme may help and may be used to define a possible, well experienced approach, based upon so called Protection Profiles. Detailed technical challenges in security have to be tested, using existing infrastructures to be tailored addressing the new purposes of mobile environments requirements.

It has become obvious that the identification of individuals is only a first step and it will prepare a possible road for future expansions towards additional scenarios for customs or in crisis management. This document is restricted to technical issues and needs further enhancements for organizational and procedural issues. It offers a first step and some technical guidance into a new, upcoming and challenging area supporting the relevant stakeholders and contributes to the protection of the citizens and the society.

9. References

[1] http://www.ants.interieur.gouv.fr/evenements/MOBIDIG-Presentation,161.html

[2] http://www.sweden.gov.se/sb/d/11627/nocache/true/a/119953/dictionary/true

[3] www.consilium.europa.eu/uedocs/cmsUpload/st00006.en09.pdf

[4] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/987&format=HTML&aged=0&language=EN&guiLanguage=en

[5] 20100416 MOBIDIG short presentation POLICE COOPERATION WG

[6] MIDAS-Project (UK, NPIA): http://www.npia.police.uk/en/10046.htm

[7] FAST-ID Project (Germany, Bundespolizei): http://www.bromba.com/press10d.htm

[8] The ‘4in1’-Project (F, ANTS)

[9] NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0, S. Orandi / R. M. McCabe, NIST, Information Access Division, Information Technology Laboratory, 08/ 2009

[10] http://www.commoncriteriaportal.org/index.html

[11] Biometric attack vectors and defences, C. Roberts, in ‘Computers & Security (2007): www.sciencedirect.com

[12] http://en.wikipedia.org/wiki/Protection_Profile

[13] http://www.commoncriteriaportal.org/thecc.html

[14] Best Network: http://www.best-nw.eu/

[15] http://www.tetramou.com/uploadedFiles/Files/Documents/Column%20Verbinding%20januari%202010%20%28Europese%20ontwikelingen%20ISI%20+%20breedband%29.pdf

10. Acronyms, Abbreviations and Definitions

AAS	*Application related Architecture Structure* (AAS)
Application related Architecture Structure	This structure distinguishes between 4 layers: - *scenario*, - *application scenario*, - *application area* and - *use case*
Application Area	An application area is an application scenario for an area such as land, sea or air
Application Scenario	Describes a scenario tailored for a specific application (such as an identification of a person or an authentication of documents)
Authentication	The process of establishing confidence in the truth of some claim. In the specific context of MOBIDIG, the validation of the mobile device (terminal authentication), the user (user authentication), the electronic document (chip authentication and passive authentication of data stored in the chip).
Authenticity	the process (evidence) that the document used for the purpose of identification or verification is not forged, expired or stolen
(I)AFIS	(Integrated) Automated Fingerprint Identification System
BAC	Basic Access Control
BCP	Border Control Point
BIG	Brussels Interoperability Group
Biometrics ID document	Any Id document which contains a chip (contact or contactless) with biometric data (images or templates) embedded.
Bluetooth	Industry standard according to IEEE 802.15.1, used for short distance wireless communication (WPAN)
CSCA	Country Signing Certificate Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Authority
CEM	Common Criteria Evaluation Methodology
CRAMM	The CCTA Risk Analysis and Management Method was created in 1987 by the Central Computing and Telecommunications Agency (CCTA) of the United Kingdom government. see: http://en.wikipedia.org/wiki/CRAMM
device	See *mobile device*
DoS	Denial of Service
EAL	Evaluation Assurance Level
EAC	Extended Access Control
EC	European Commission
eID	Electronic Identity Document
eIDM	Electronic Identity Management
EFFISEC	Efficient integrated security checkpoints (a project running under FP7) (http://www.effisec.rdg.ac.uk/project.htm)
Electronic ID document	Any ID document which contains a chip (contact or contactless) with any biometric data (images or templates) embedded.
(Electronic) identity token	a physical device as an electronic ID document (ePassport, identity card, smart card), or a hardware token, a hard token, an authentication token, *USB* token, cryptographic token storing data for identification or authentication purposes in digital or electronic form
ESO	European Standardisation Organisation
EU-MS	European Member States
FAR	False Acceptance Rate (performance criteria, often used in biometrics)
FRR	False Rejection Rate (performance criteria, often used in biometrics)
FORERUNNER	European Project for Radio Communication for Law Enforcement

3G/4G	3rd / 4th Generation in communication
GPS	Global Position System
Handheld device	Portable technical device intended to perform non stationary ID checks which is not tethered to a car or to hardwired to a much larger system
IBTL	Interoperability and biometrics test laboratory
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technology
ID	Identification and/or identity
ID	Identity document
Identification	- Process, by which, a person's identity is established - A task were the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity
Identity	Set of characters that individualize a person.
Identity check	Action in order, in a defined legal framework, to process to the verification of the data contained in an ID document by a law enforcement or border control officer, with or without any device.
IS	Inspection System
ISO	International Standardisation Organisation
ITS-System	frequently used to refer to the interaction between people, algorithmic processes, data and technology
JRC IPSC	Joint Research Centre, Institute for the Protection and Security of Citizen
MESH	Mesh networking is a type of networking wherein each node in the network may act as an independent router, regardless of whether it is connected to another network or not (e.g. often used for sensor networks)
MOBIDIG	European Mobile Identity Interoperability Working Group
MOBIDIG Technical WG	One of 4 WG maintained by MOBIDIG
Mobile device / Mobile ID device	Portable technical device intended to perform non stationary ID checks. The Mobile ID device should be viewed in the context of a portable biometric acquisition station – one that is not intended to be stationary and hardwired to a much larger system. A device physically attached to a computer located in a vehicle that acquires biometric samples may also be considered as a Mobile ID device. It may consist of an untethered device used to capture one or more biometric samples from a subject.
Mobile ID check	Action taken in order to establish a person's identity by means of using mobile devices.
MRTD	Machine Readable Travel Documents
MRZ	Machine Readable Zone
NFC	Near Field Communication
OCTAVE ®	Operationally Critical Threat, Asset, and Vulnerability Evaluation
P3P	Platform for Privacy Preferences Project.
PDA	Personal Digital Assistant
PKD	Public Key Data base
PMR	Professional Mobile Radio
PP	Protection Profile
RFID	Radio Frequency Identification
SAR	Security Assessment Requirement
SFR	Security Function Requirement
USB	Universal Serial Bus

Use case	A use case is a specific concrete case for a selected application area such as identification of person in a bus, or the check for authenticity (authentication) of an e-driver licence or ePassport or the verification of a passenger on plane or on board of a boat (for .g. for immigration purposes)
scenario	a composition / a set of application scenarios building one common scenario
ST	Security Target
STA	Security Technology Assessment: unit at the JRC IPSC
Stationary mobile device	Mobile device which is placed for a non permanent duration in a fixed position for a specific use, and which can be removed for use at another location.
TETRA	Terrestrial Trunked Radio
Tetrapol	Terrestrial Trunked Radio for application for police
token	See: *electronic identity token*
Verification	A task were the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled biometric data (images or templates)
VPN	Virtual Private Network
WG	Working group

European Commission

EUR 24548 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Technical challenges for identification in mobile environments
Authors: Klaus Keus, National Detached Expert at the JRC and Jan Loeschner, JRC

Luxembourg: Publications Office of the European Union
2010 – 32 pp. – 21 x 29,7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-17049-2
doi:10.2788/26072
Abstract

This report describes some main technical challenges and requirements for identification of individuals in mobile (i.e. non-stationary) environments as e.g. required by the “European Mobile Identification Interoperability Group” (MOBIDIG). It is intended to support relevant stakeholders as law enforcement agencies or immigration offices, active in the area of identification of individuals in mobile environments. It offers some guidance for future technical work at the MOBIDIG to be respected in their work plan.

Furthermore, it may be used as a first orientation for the general future work for identification in mobile environments using digital or electronically stored data. After the introduction and some background of MOBIDIG and its policy context, the document presents the intention, main objectives and some information about the scope of work of the group. The following proposals, suggestions and recommendations presented are explicitly focusing on technology. Organizational and procedural issues are out of focus of this document and need to be addressed separately in further documents.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

LB-NA-24548-EN-C

JRC
EUROPEAN COMMISSION

Publications Office

ISBN 978-92-79-17049-2

9 789279 170492