

Project Number: **621021**
Acronym: **PIDaaS**
Title: **Private Identity as a Service**
Call (part) identifier: **CIP-ICT-PSP-2013**
Start date: **01/07/2014**
Duration: **30 months**

D4.3

Intermediary Users Documentation

Nature¹: **R**
Dissemination level²: **PU**
Due date: **31/12/2015**
Date of delivery: **31/12/2015**

Partners involved:

- BANTEC CONSULTORES INICIATIVAS EMPRENDEDORAS SL (BANTEC)
- EURECAT - CENTRE TECNOLÒGIC DE CATALUNYA (EURECAT)
- RICOH SPAIN IT SERVICES SLU (RICOH)
- HOGSKOLEN I GJOVIK (GUC)
- UNIVERSITY OF KENT (UKENT)

Authors:

Juan Caubet (EURECAT), Diego Delgado (EURECAT), Pau Bellorbi (RICOH), Iván Jiménez (BANTEC), Guoqiang Li (GUC) & Oscar Miguel-Hurtado (UKENT)

¹ R = Report, P = Prototype, D = Demonstrator, O = Other

² PU = Public, PP = Restricted to other program participants (including the Commission Services), RE= Restricted to a group specified by the consortium (including the Commission Services), CO = Confidential, only for members of the consortium (including the Commission Services)

Revision history

Revision	Date	Author	Organisation	Description
0.1	2015-11-03	Oscar Miguel-Hurtado / Guoqiang Li	UKENT/GUC	Initial draft version
0.2	2015-11-12	Oscar Miguel-Hurtado / Guoqiang Li	UKENT/GUC	Work distribution
0.3	2015-12-10	Oscar Miguel-Hurtado / Guoqiang Li	UKENT/GUC	Contributions Integration
0.4	2015-12-10	Oscar Miguel-Hurtado / Guoqiang Li	UKENT/GUC	Contributions Integration
0.5	2015-12-16	Oscar Miguel-Hurtado / Guoqiang Li	UKENT/GUC	Contributions Integration
0.5.5	2015-12-18	Iván Jiménez / Juan Caubet / Guoqiang Li	BANTEC/EURECAT/GUC	Contributions Integration
0.6	2015-12-23	Oscar Miguel Hurtado	UKENT	Final draft version
0.7	2015-12-24	Oscar Miguel Hurtado	UKENT	Final Version

Disclaimer

The work associated with this report has been carried out in accordance with the highest technical standards and the PIDaaS partners have endeavoured to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this report (or any further consolidation, summary, publication or dissemination of the information contained within this report) and/or the connected work and disclaim all liability for any loss, damage, expenses, claims or infringement of third party rights.

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Abstract

Numerous internet services require the users to authenticate themselves. More and more users are unable to cope with memorizing the numerous secure passwords. In this context, the use of biometric authentication can produce relief to the users. Many mobile devices contain input devices that can be used for capturing biometric data such as voice data or face images. The objectives of the PIDaaS project are to create and to field-test an innovative identity management service relying on biometric traits as one of the most important factors for identity assurance and including other meta-data (obtained from hardware, software and network) to better define the level of certainty of the authentication request. This document states clear information for the end-users to be successfully prepare the evaluation of the PIDaaS Platform during the piloting phases.

Contents

1	Introduction	9
1.1	Project objectives	9
1.2	Document scope and outline	9
2	PIDaaS Platform overview	10
3	Usability, Security and Performance Evaluation Introduction	12
3.1	Usability evaluation	12
3.2	PIDaaS HBSI metrics.....	13
3.2.1	PIDaaS HBSI framework metrics	13
3.2.2	PIDaaS HBSI presentation metrics	14
3.3	Security and biometric performance evaluation	17
3.3.1	Security analysis regarding PIDaaS authentication protocol.....	17
3.3.2	Security analysis regarding biometric template protection scheme.....	17
3.3.3	Biometric performance evaluation.....	18
4	End-Users pilot introduction.....	19
4.1	Introduction of user account association and authentication delegation.....	19
4.2	Phase 1, internal pilot.....	20
4.3	Phase 2, small scale pilot	21
4.4	Phase 3, large scale pilot	21
5	Implement delegated authentication in their websites from Service Provider point view	23
5.1	Association between Service Provider User Accounts and PIDaaS Accounts	25
6	Mobile Platforms descriptions	28
6.1	PIDaaS Mobile platform HW requirements.....	28
6.1.1	PIDaaS Mobile iOS HW requirements	28
6.1.2	PIDaaS Mobile Android HW requirements	29
6.2	PIDaaS Mobile platform distribution.....	29
6.2.1	PIDaaS Mobile platform internal distribution: TesfFairy.....	29
7	Select target population for each phase	33
8	Training material for participants, brief introduction of D4.4.....	34
8.1	Registration in PIDaaS Platform.....	34
8.2	Login in PIDaaS Mobile App	36
8.3	Replay to an authentication request	37
9	Usability, privacy and security performance analysis, brief introduction of D4.5 ...	39
	References	40

List of figures

Figure 1 PIDaaS Pilot Lab Architecture Diagram	10
Figure 2 HBSI model	12
Figure 3 HBSI evaluation method.....	13
Figure 4 HBSI presentation categories.....	14
Figure 5 Users' accounts association	19
Figure 6 Delegation of Authentication.....	20
Figure 7. PIDaaS delegated authentication flow	24
Figure 8: Association process between a PIDaaS account and a SP account	27
Figure 9: TestFairy Tester Mobile Registration Request email	30
Figure 10: TestFairy Tester Mobile Registration process	30
Figure 11: TestFairy web interface Dashboard for Mobile Beta Apps distribution to testers	31
Figure 12: TestFairy Mobile Beta App distribution email to tester	32
Figure 13 Start-up page of registration process	34
Figure 14 Interfaces for typing PIN and for selecting biometrics modality.....	35
Figure 15 Interface for voice registration.....	35
Figure 16: Interfaces for face registration	36
Figure 17 Last page of user registration.....	36
Figure 18 Start-up page of user login.....	37
Figure 19 Voice and Face authentication interfaces	37
Figure 20 Authentication request message in PIDaaS Mobile App.....	38
Figure 21 Authentication request details.....	38

List of abbreviations

AAI	Authentication and Authorisation Infrastructure
A-BTPS	Adapted Biometric Template Protection Scheme
API	Application Programming Interface
APNS	Apple Push Notification Service
BCH	Bose-Chaudhuri-Hocquenghem
BTPS	Biometric Template Protection Scheme
CA	Certification Authority
CC	Cross Comparator
CI	concealed interaction
DB	Database
dHBSI	dynamic Human Biometric Sensor Interaction
DI	defective interaction
DIS	Draft International Standard
DOS	denial of service
EAL	Evaluation Assurance Level
ECCR	Equal Cross-Comparison Rate
EER	Equal Error Rate
FAR	False Accept Rate
FCMR	false cross match rate
FNCMR	false non cross-match rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
FTD	failure to detect
FTE	Failure To Enrol
FTP	Failure to Process
FTX	failure to extract
GCM	Google Cloud Messaging
GPS	Global Positioning System
HBSI	Human-Biometric-Sensor Interaction
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JVM	Java Virtual Machine
LBLDA	Local Binary Linear Discriminant Analysis
LDA	Linear Discriminant Analysis
LGIP	Local Gradient Increasing Pattern
LMP	Life Management Platform
MFCC	Mel Frequency Cepstral Coefficient
PCA	Principal Components Analysis
PIDaaS	Private Identity as a Service
PIN	Personal Identification Number
PKI	Public Key Infrastructure

PNS	Push Notification Service
PT	Protected Template
SAS	successfully acquired samples
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSO	Single Sign On
URL	Uniform Resource Locator
VAD	Voice Activity Detection
XML	Extended Markup Language

1 Introduction

In this section we will summarize the PIDaaS Project objectives in Section 1. It will be followed by Section 1.2 where the scope and the outline of the deliverable D4.3 will be detailed.

1.1 Project objectives

The objectives of the PIDaaS project are to create and to field-test an innovative identity management service relying on biometric traits as one of the most important factor for identity assurance and including other meta-data to better define the level of certainty of an authentication request.

The PIDaaS project is based on three key technologies: the biometric authentication technology which bring biometrics security to the authentication process, the biometric template protection scheme which enhance security and provide privacy to the biometrics traits and the Life Management Platform which allow user to take control of the use of their biometric information.

1.2 Document scope and outline

The scope of the deliverable 4.3 is to provide to the end-users a brief and non-technical overview of the PIDaaS Pilots that will be carry out at WP5.

The PIDaaS Platform and its main components will be summarized at Section 2. This overview will be followed by an introduction of the Usability, Security and Performance Evaluation that will be carried out at the Pilot phases (Section 3). This introduction will help end-users to better understand the goals of these evaluations.

The Section 4 will provide guidelines for the setting of the Pilot phases in order to proceed with the data collection experiment. It will explain the three data collection phases that will be required: internal pilot, small scale pilot and large scale pilot. In order to start this data collection experiment, Section 5 will explain how to implement the authentication delegation and Section 6 will introduce the PIDaaS Mobile App and define the mobile hardware requirements. Finally, at Section 7 we will provide advices for selecting the target population for each phase.

Section 8 and 9 will briefly introduce the next two deliverables:

- D4.4 which will provide to the service providers training material for the data collection experiment, and
- D4.5 which will provide details of how the PIDaaS Platform will be analysed in terms of usability, security and performance.

2 PIDaaS Platform overview

A simplified PIDaaS Platform architecture is depicted in Figure 1 from a technical perspective.

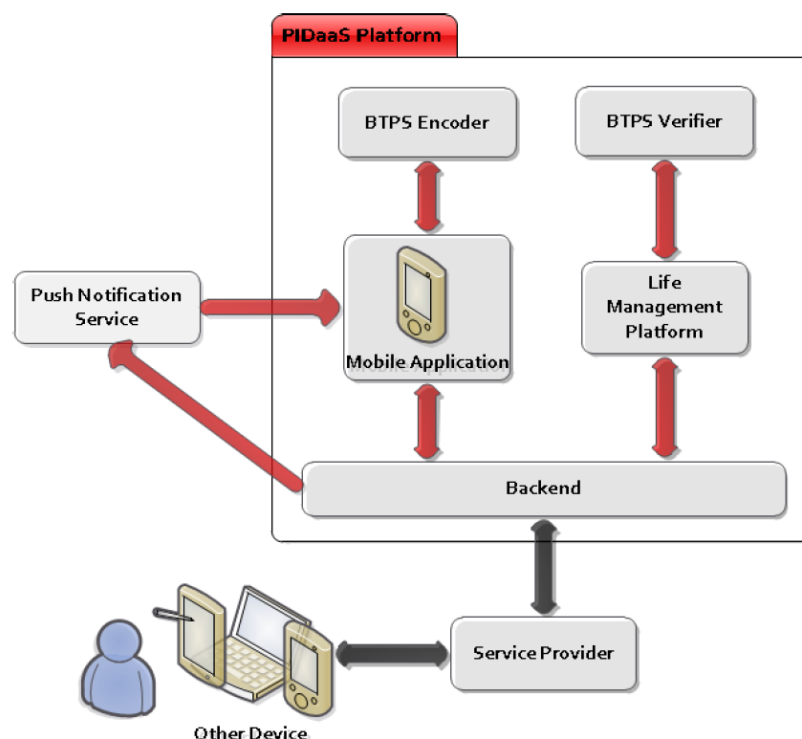


Figure 1 PIDaaS Pilot Lab Architecture Diagram

The PIDaaS Platform is composed by the following components:

- **The PIDaaS Mobile App:** this app will be installed on the user's mobile and its main use will be to capture and process the biometrics samples (voice and face). The PIDaaS Mobile App will also be used to get user's register in the PIDaaS Platform and to receive authentication requests from the service providers. These authentication requests will be generated at the authentication delegation process into PIDaaS from the service providers.
- **The Life Management Platform (LMP):** The LMP will provide the management of the biometrics pseudo identities (renovation, cancelation, expiration dates). Through this platform, the user will be also able to get a historical record of where (which service provider) and when (date and time) their data have been used for authentication. This platform is built on open source technologies and use the Security Assertion Markup Language (SAML2.0) as a standardized protocols for authentication and authorization delegation. LMP also includes a Certification Authority (CA), which is able to issue digital certificates for both PIDaaS users and components. In this way, all the components for the PIDaaS Platform (LMP, Backend Service and Mobile application) are authenticated before to stablish a secure connection.

- **Biometric Template Protection Schemes (BTPS):** The Biometric Template Protection Schemes technology provides two main components to the PIDaaS Platform. The BTPS Encoder is integrated within the PIDaaS Mobile App and allow this app to generate pseudo identities from the biometric samples (voice and face) captured using the mobile sensors (microphone and front camera). This component will not store or share any biometric data, enhancing the security and privacy of the users. The second BTPS component, named BTPS Verifier, is located at the Life Management Platform. This component is responsible of the comparison process during the authentication requests. It will compare the pseudo identity created from the biometric data captured at the authentication requests with the pseudo identity created from the biometric data captured at the registration phase.
- **The PIDaaS Backend:** the PIDaaS Backend provide a gateway to both PIDaaS Mobile and Service Providers to access the PIDaaS Services located at the LMP component.

The PIDaaS Platform will be integrated at the Service Providers work flow in order to delegate the authentication in their websites. This delegation will require previously an enrolment of the service provider's users at the PIDaaS Platform.

3 Usability, Security and Performance Evaluation Introduction

Both from users and service provider's point of view, the performance of the biometric authentication will be a key factor in the PIDaaS Platform success. Service provider needs to increase security and accessibility through seamless authentication process. On the other hand, users want to be sure that their personal and biometric data and the access to their service providers is secured, avoiding impersonations while assuring privacy.

The biometric performance commonly is assessed under laboratory conditions. In these conditions, the users are guided on how to use the device, and the environmental conditions (i.e. noise and ambient light) are tightly controlled. This conventional evaluation focus on error rates in authentication using metrics such as 'false rejection rate' and 'false acceptance rate' relating to legitimate rejection and illegitimate access respectively. These metrics provide statistics on how well the algorithmic/sensor implementations performs, but do not indicate how the system performance can be affected by how the user interact with the system.

Accurately understanding how a user interacts with a biometric implementation (especially in mobile devices where the user interactions can vary greatly among the population) can lead to important final system performance enhancement and can improve significantly both the user's experience and system throughput.

3.1 Usability evaluation

As presented in previous deliverables, the HBSI framework [1] models and provides metrics to evaluate the interactions between the human (users of the biometric solution), the sensor (in our case the mobile device) and the biometric system (the PIDaaS Platform), Figure 2:

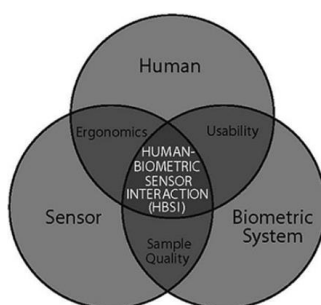


Figure 2 HBSI model

The human-sensor portion is related to how the users present their biometrics characteristics to the sensor. The sensor in the PIDaaS Mobile App will be the microphone and the front camera of the mobile devices where the PIDaaS Mobile App is installed. The analysis of this interaction will help us understand how to better guide the users in order to obtain better quality in the biometrics samples captured.

The human-biometric system component deal with how users interact with the PIDaaS Platform, mostly through the PIDaaS Mobile App interface. In this case we, the usability evaluation will help us to design a better user-centric interface.

The sensor-system portion is measured through the quality of the biometrics captured samples, let us know if these sample have enough information in order to produce accurate verifications.

In also worth to highlight that all these variables (ergonomics, usability and sample quality) are impacted by the overall environmental conditions in which they are collected.

3.2 PIDaaS HBSI metrics

The usability analysis included in the HBSI model considers the three main parameters proposed by the ISO 13407:1999 [2]: satisfaction, efficiency and effectiveness. The ergonomics in the HBSI includes cognitive (what users knew about how to use the system, how users learn to use the system, and how user remember how to use the system) and physical categories (the percentage of users that can use the capture sensor). The signal processing includes sample quality metrics and processing capability (i.e. number of feature extraction errors).

3.2.1 PIDaaS HBSI framework metrics

Figure 6 depicts the HBSI metrics of a complete usability evaluation within this framework:

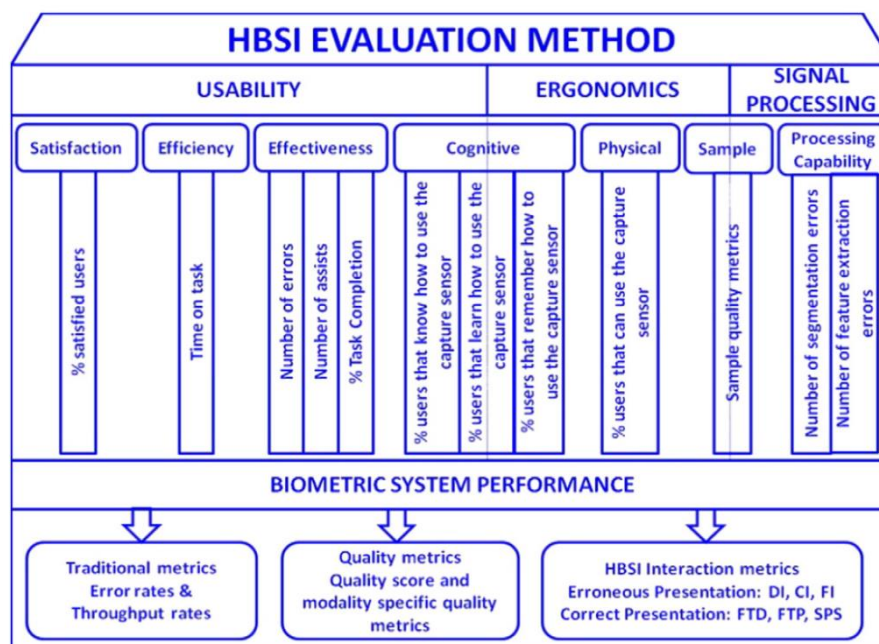


Figure 3 HBSI evaluation method

Using the time-stamp information obtained from the log of the user's interaction events during the pilot phases, the HBSI metrics will be calculated as follows:

- Efficiency: The time spent on performing an authentication request
- Effectiveness: The task completion rate by users.
 - Number of errors detected by test operator

- Number of assists
- % Task completions
- Cognitive:
 - Intuitive-ability (% of users that know how to use the system)
 - Learnability (% of users that learn how to use the system)
 - Memorability (% of user that remember how to use the system):
- Sample Quality Metrics:
- Signal processing:
 - Number of segmentation errors
 - Number of feature extraction errors
 - Time to process samples

3.2.2 PIDaaS HBSI presentation metrics

As a results of the application of the HBSI model, different metrics will be obtained. These metrics will allow to have a holistic view of the system performance in terms of usability and algorithm throughput rates. These metrics include traditional biometric metrics (EER, FAR, FRR), quality metrics and HBSI presentation metrics (DI, CI, FI, FTD, FTP, SAS).

The HBSI presentation metrics are determined by the type of presentations the users make, and their categorisation depend on whether the user made a correct or incorrect presentation. The user's presentations will be labelled following the HBSI framework categories:

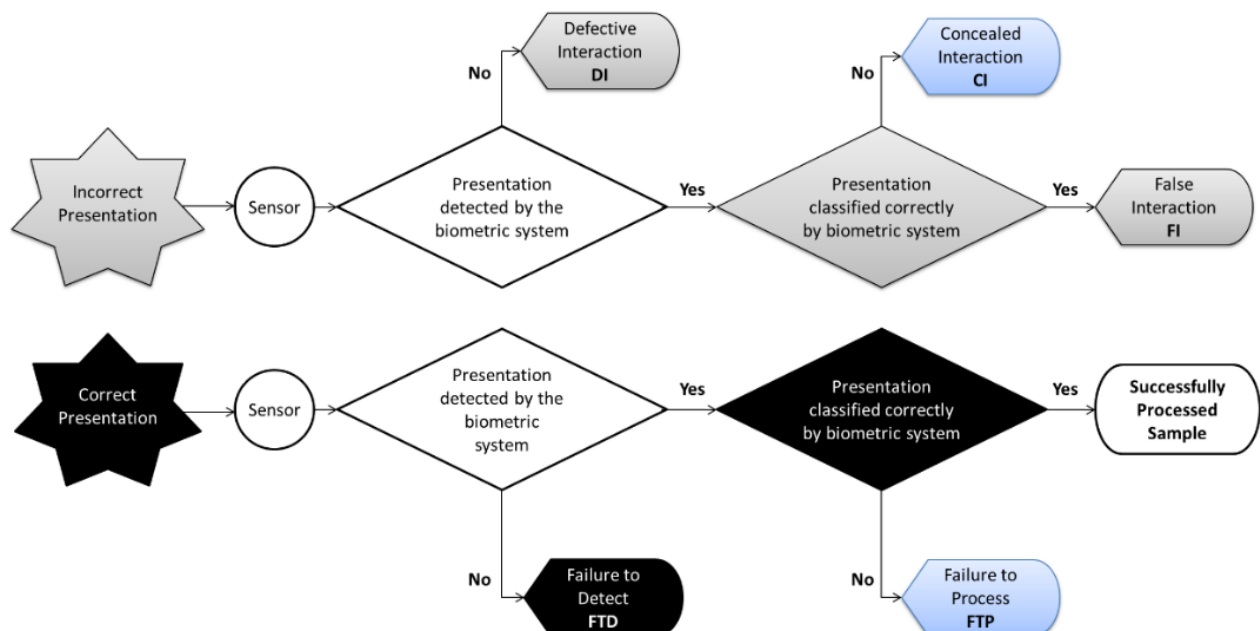


Figure 4 HBSI presentation categories

A presentation in PIDaaS consists on either a voice or a face sample. A correct and incorrect presentation are defined as:

1. **Correct presentation:**

- a. **Voice:** A correct presentation occurs when the user repeat, synchronized with the PIDaaS Mobile App, the exactly same numbers as they are presented in an understandable way, with enough loudness and under a reasonable noise level.
- b. **Face:** A correct presentation occurs when the user places the head within the shadow-picture-frame. The face is clearly visible, without any part covered or occluded and the light conditions are uniform over the image without any shadows.

2. **Incorrect presentation:**

- a. **Voice:** in a general way, anything that doesn't fit the correct voice presentation definition. An incorrect presentation might be due to the following reasons:
 - i. High noise level
 - ii. The user did not repeat all the number in the sequence
 - iii. The user did no repeat the right numbers in the sequence
 - iv. Interruptions
 - v. The user occluded the microphone.
- b. **Face:** in a general way, anything that doesn't fir the correct face presentation definition. An incorrect presentation might be due to the following reasons:
 - i. Head no fully place within the shadow-picture-frame.
 - ii. Strong lights from the background making the face no visible
 - iii. Shadows over the faces
 - iv. Face partially occluded by clothes or wearings.

Once the incorrect and correct presentations are defined, the presentation would be classified into one of the six HBSI categories:

1. **Defective Interaction (DI):** A defective interaction occurs when a user makes an incorrect presentation that is not detected by the biometric system.
 - a. **Voice:** not possible, voice records are always captured, whether the user is talking or not.
 - b. **Face:** not possible, face images are always captured (as long as they press the PICTURE icon), whether the users place the face to the front camera or not.
2. **Concealed Interaction (CI):** System CI's are the result of an erroneous presentation that contains unrecognizable features which are subsequently recorded as a successfully acquired sample, and therefore further processed by the system into the comparison engine against the user's template.

- a. **Voice:** incorrect presentation that is not classified correctly by voice activity detection module (VAD). This presentation, although incorrect, will be send to the server to be compared with the user's biometric template.
 - b. **Face:** As there is not any quality checking for face verification, all the incorrect presentation will fall into this category.
3. **False Interaction (FI):** FI occurs when a user presents their biometric features to the biometric system, which are detected by the system and is correctly classified by the system as erroneous due to a fault or errors that originated from an incorrect action, behaviour, or movement executed by the user.
 - a. **Voice:** the erroneous presentation is classified correctly by the VAD and not further processed for the system. The PIDaaS App will ask the user to present again another voice sample.
 - b. **Face:** as there is not any quality checking for face authentication, none interaction will fall into this category.
4. **Failure to Detect (FTD):** a FTD involves a correct presentation to the sensor but not detected by the biometric system, and therefore, not acquired by the sensor. Due to the implementations details of PIDaaS Mobile App, there won't be any correct presentation labelled as FTD as the sensor will always record the sound or take the picture.
5. **Failure to Process (FTP):** After a correct presentation is made to the sensor, and it is detected by the sensor, and acquisition occurs, the system attempts to create biometric features from the collected sample. In the general biometric model, this occurs in the signal processing module. A failure to process (FTP) is concerned with samples from the data collection module that are unable to be processed completely.
 - a. **Voice:** After a correct presentation is made to the sensor, and recorded, the system attempts to create the i-vector. A failure to process (FTP) will occur when this attempt is unsuccessful. This failure can come for the transmission of the voice sample to the server or from the signal processing module at the server side. An error should be logged either at the device side if it comes from the transmission, or at the server-side if is due to the signal processing module.
 - b. **Face:** same as in Voice. However, as there is not any algorithm implemented for face authentication, a failure to extract won't ever occur.
6. **Successfully Processed Sample (SPS):** a SPS is a correct presentation that is recorded by the biometric system and successfully processed as an i-vector. The biometric sample meets system specifications, allowing for the i-vector to be created and further processed to a BTPS pseudo identity.

To be able to categorize the user presentations, the following information is needed:

1. Classify the presentation as correct or incorrect. This task is made manually by the data collection operator.
2. Response of the voice activity detection (VAD) module.
3. Response of the server side that the i-vector has been successfully created.

3.3 Security and biometric performance evaluation

3.3.1 Security analysis regarding PIDaaS authentication protocol

PIDaaS authentication protocol is the cornerstone of PIDaaS platform to provide a secure mechanism to verify users' identity by using their personal information including some geographic information and biometric data. Besides the security analysis related to the biometric verification, it is also essential to analyze the security of this authentication protocol from some other aspects:

1. Network mechanism to guarantee a secure channel for communication among end-users, service providers and PIDaaS platform;
2. Data protection mechanism related to the LMP database;
3. Vulnerability analysis regarding denial of service (DOS) attack;
4. Protocol analysis against the common network attacks, *e.g.*, man-in-middle attack, impersonation attack, masquerade attack, etc.

3.3.2 Security analysis regarding biometric template protection scheme

In accordance with the ISO/IEC 24745:2011 [3], the security analysis related to the biometric data will be carried out from analyzing two perspectives: irreversibility and unlinkability.

In specific, irreversibility will be investigated from the following three aspects:

- Full-leakage irreversibility: the difficulty of determining, exactly or with tolerable margin, from a PT, the biometric sample(s) or features used during enrolment to generate that PT.
- Authorized-leakage irreversibility: the difficulty of determining a biometric sample(s) or features from a PT that would “match” the unprotected enrolment data in a disjoint unprotected system.
- Pseudo-authorized-leakage irreversibility: the difficulty of determining, exactly or to a high degree of similarity, from a protected template, the biometric sample(s) or features that match the protected template but would not “match” the unprotected enrolment data in a disjoint unprotected system.

And the unlinkability analysis will be evaluated by reporting three metrics: false cross match rate (FCMR), false non cross-match rate (FNCMR) and equal cross-comparison rate (ECCR) defined.

According the explanation in [3], we assume PT_1 and PT_2 denote two protected templates derived from samples b_1 and b_2 , respectively. In first instance, $b_1 = b_2$. However, some schemes cannot provide unlinkability if two enrolment samples are equal, hence two different measurements from the same characteristic should be used. Let the binary operator \sim denote that two PT s are a mate pair and $\not\sim$ that they are not. Let f be the heuristic function used for evaluation by a cross-comparator CC_f . The CC_f takes as input two PT s and some parameters p , like a decision threshold, and outputs 1 if the input templates are evaluated by CC_f as a mate pair and zero otherwise.

Let DB be a particular database over which a cross-comparator CC_f is evaluated. Then M_{DB} denotes the subset of all mate pairs from DB and NM_{DB} the subset of non-mate pairs:

$$M_{DB} = \{(i, j) \mid i, j \in DB \wedge i \sim j\}$$

$$NM_{DB} = \{(i, j) \mid i, j \in DB \wedge i \not\sim j\}$$

Then the false cross-match rate (FCMR) and the false non-cross-match rate (FNCMR) can be defined as:

$$FCMR_f = \#\{x \in NM_{DB} : CC_f(x) = 1\} / \#NM_{DB}$$

$$FNCMR_f = \#\{x \in M_{DB} : CC_f(x) = 0\} / \#M_{DB}$$

The equal cross-comparison rate is defined as the point where $FCMR_f = FNCMR_f$.

3.3.3 Biometric performance evaluation.

Regarding biometric recognition accuracy, we follow some commonly used metrics to evaluate the performance during our experiments at difference phases. These metrics have been defined in ISO/IEC 2382-37 [4] in order to evaluate the performance of a biometric system. In brief, the following metrics have been selected:

- False Match Rate (FMR) is the proportion which non-authorized user are falsely recognized during verification process;
- False Non-match Rate is the proportion which genuine user are falsely not recognized during verification process;
- False Acceptance Rate (FAR) is the rate that a non-authorized user is accepted to access the system;
- False Rejection Rate (FRR) is the rate that a genuine user is rejected to access the system. There are several reason to cause false rejection, such as failed to capture the biometric data, system failure, etc;
- Equal Error Rate is the value where FMR and FNMR are equal.

FMR and FNMR are designed to reflect the accuracy at algorithm level. FAR and FRR are designed to reflect the accuracy at system level. Thus FMR and FNMR as well as EER will be adopted to evaluate the accuracy of adapted BTPS evaluation. FAR and FRR will be used to evaluate the accuracy of PIDaaS system.

4 End-Users pilot introduction

This chapter will give a recommendation for the three end-users (e-Citizen, e-Health, and e-Commerce) how to establish their own data collection experiment. This recommendation consists of three phases: internal pilot, small scale pilot and large scale pilot. The details of these phases will be discussed in the sub sections in this chapter. Before introducing these phases, it is necessary to have the basic logic behind the authentication delegation, association between service providers and PIDaaS accounts from the user's perspective, where this user refers to the customers of the service provider. The following section briefly describe this logic.

4.1 Introduction of user account association and authentication delegation

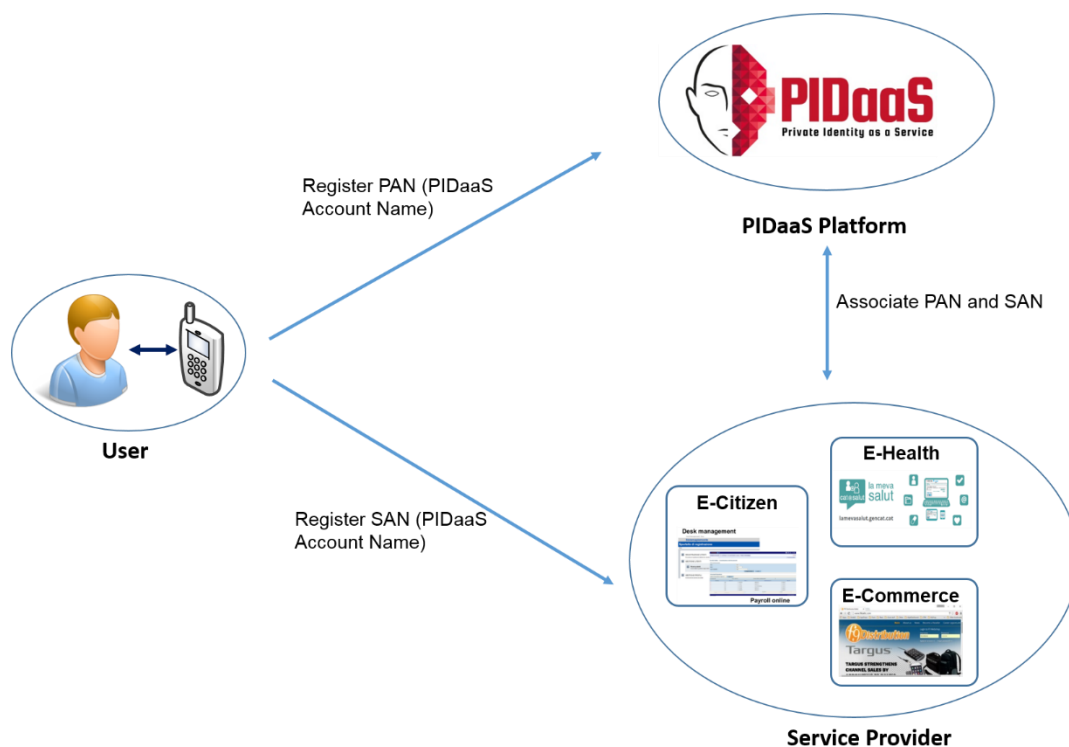


Figure 5 Users' accounts association

Before associating PAN (PIDaaS Account Name) and SAN (Service Account Name), the user needs to register a PIDaaS Account via the PIDaaS Mobile App. If the user already has the account from the service provider, the association between PAN and SAN can be configured through a website provided by a specific service provider. If the user doesn't have a service provider account yet, the user can register an account via a service provider's website and associate with PAN accordingly. Figure 5 illustrates the relation between PAN and SAN.

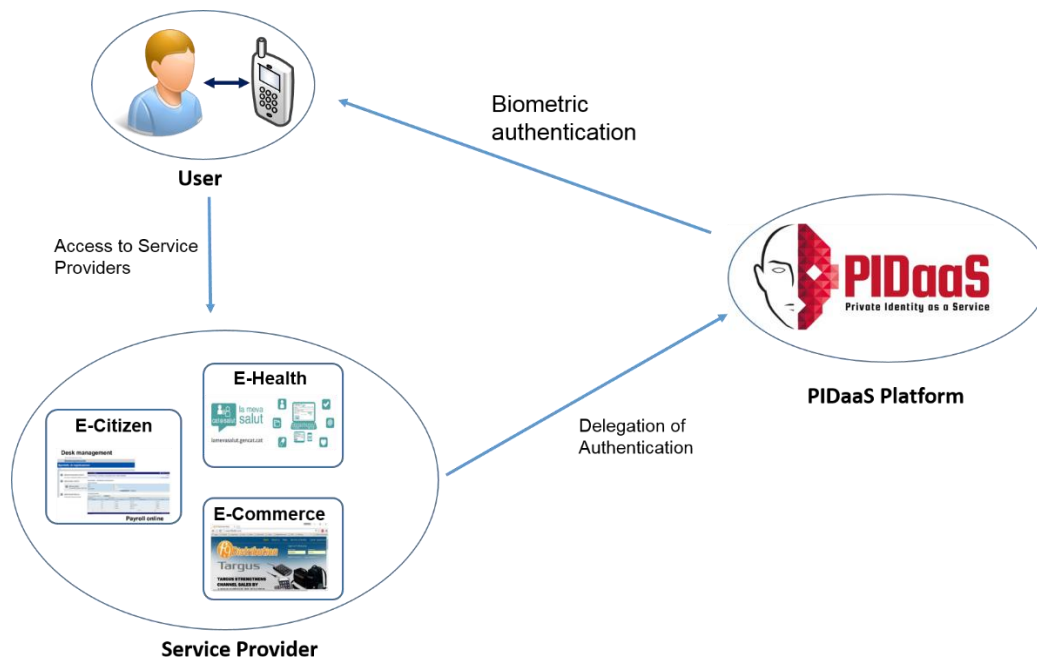


Figure 6 Delegation of Authentication

After the user's account association, PIDaaS Platform will be able to authenticate the user's identity by using his/her biometric information.

Figure 6 shows a brief workflow of the authentication delegation. The user will initiate the authentication process when he/she is going to access a service. The service provider will delegate this authentication process to the PIDaaS Platform who stores users' identity information. Then the PIDaaS Platform will communicate with the user to carry out an authentication process which requires the user to capture his/her biometric information by using his mobile device and the PIDaaS Mobile App. At the end, the PIDaaS Platform will inform the corresponding service provider about the authentication result. The service provider will grant or reject user's access request based on this authentication result.

4.2 Phase 1, internal pilot

Phase 1 is defined as an internal pilot which can be considered as a preparation step before carrying out the actual data collection. This phase is recommended to be operated by at least 2 members from the project management team. The main purpose of phase 1 is to check all functionalities have been well implemented and work as expected. These functionalities include the following aspects but not limited to these:

1. Make sure all the mobile devices which are going to install PIDaaS Mobile App will meet the following requirements:
 - a. iOS device: iPhone 5/5C/5S, 16:9 aspect/ratio device, with iOS 7 or higher [iOS8.x]; iPod Touch 5 (5th generation) with iOS7 (or higher [iOS8.x]); iPhone6 with iOS8.x; iPhone6+ with iOS8.x.
 - b. Android device: Android mobile phone with Android v4.0 (or higher).

2. Make sure to obtain the latest version of PIDaaS Mobile App from BANTEC;
3. Install PIDaaS Mobile App in some of the mobile devices, at least one device from each model of mobile device, and check if all these mobile devices can successfully install PIDaaS Mobile App;
4. Create a PIDaaS account by using one device from each model of mobile device;
5. Subscribe a service provider;
6. Log into the PIDaaS account using the PIDaaS Mobile App;
7. Confirm an authentication request from the service provider;
8. Renew the biometrics templates;
9. Check that all interfaces of the PIDaaS Mobile App can be displayed properly.

4.3 Phase 2, small scale pilot

Phase 2 is defined as a small scale pilot which will collect data from selected end-users. The main purpose of this phase is to obtain the feedbacks from the actual users in order to improve the PIDaaS Platform and PIDaaS Mobile App before deploying the PIDaaS Mobile App to all participants.

The tasks which need to be carried out in this phase includes:

1. A feedback questionnaire which will collect participants' previous experience about smart-devices and biometrics;
2. A feedback questionnaire which will collect basic participants' demographics such as gender, age, native language, handedness, etc.;
3. A testing form which will record any software errors encountered during the data collection period;
4. Analyse the usability, privacy and security performance results and define the update priorities in order to improve the performance of the PIDaaS Platform. This task needs to be accomplished by the PIDaaS Platform developers.
5. Analyse the feedback questionnaires and testing form, and define the priorities for those valuable comments. This task needs to be accomplished by the PIDaaS Platform developers and technical support from the service providers.
6. Fix the software errors encountered during the data collection period, and improve the PIDaaS Platform according to the priorities defined in Step 4.

4.4 Phase 3, large scale pilot

Phase 3 is defined as a large scale pilot which will invite all selected end-users' participants to use PIDaaS Platform as an authentication mechanism when they want to access a specific service. The main purpose of this phase is to improve PIDaaS Platform in terms of the usability and security by collecting the feedback from all actual users and carrying out the usability, privacy and security evaluations.

This phase will help PIDaaS Platform developers to produce a stable, secure and user-friendly PIDaaS Platform including PIDaaS Mobile App. Thus the tasks needed to be carried out in this phase will remain as same as designed in the phase 2. These tasks are:

1. A feedback questionnaire which will collect participants' previous experience about smart-devices and biometrics;
2. A feedback questionnaire which will collect basic participants' demographics such as gender, age, native language, handedness, etc.;
3. A testing form which will record any software errors encountered during the data collection period;
4. Analyse the usability, privacy and security performance results and define the update priorities in order to improve the performance of the PIDaaS Platform. This task needs to be accomplished by the PIDaaS Platform developers.
5. Analyse the feedback questionnaires and testing form, and define the priorities for those valuable comments. This task needs to be accomplished by the PIDaaS Platform developers and technical support from the service providers.
6. Fix the software errors encountered during the data collection period, and improve the PIDaaS Platform according to the priorities defined in Step 4.

5 Implement delegated authentication in their websites from Service Provider point view

The main service provided by PIDaaS is the delegated authentication. This service is performed using the Security Assertion Markup Language 2.0 (SAML 2.0) [6] protocol. SAML protocol follows a client-server model, in which SP acts as the SAML consumer and the PIDaaS Platform acts as the SAML authority (Identity Provider (IDP)). This is an XML-based protocol that uses security tokens which contain assertions to pass information about users between a SAML authority and a SAML consumer, and allows web-based authentication and authorization processes. The SAML authority issues SAML assertions, which are package of information that supplies zero or more statements. To accomplish that, SP must implement the following SAML 2.0 main client functions:

- Build and send to PIDaaS a SAML authentication request.
- Receive and validate from PIDaaS a SAML assertion (authentication statement).

In a first step, all SPs need to be registered within the PIDaaS Platform before to be able to request the authentication of a user. To this day, the registration process means manual exchange of SAML Metadata. This metadata tells the SP where the PIDaaS's services can be found on the Web, and what kind of message (Binding) it uses. For PIDaaS, SPs provide the URL where the user expects to go after a successful authentication. Both parties have also to provide the public certificates which will be used to check message signatures and encrypt message content.

From the point of view of SPs, the SAML authentication process consists of seven steps, including the moment when the user decides to use PIDaaS to authenticate him:

- The "*Login with PIDaaS*" button is clicked by the user.
- That user action generates an HTTP Request https://ip.address.of.service.provider/pidaas_samlso to SP itself.
- Then SP builds the SAML authentication request and redirects the user browser to the PIDaaS Authentication Web:
<https://ip.address.of.pidaas/samlso?SAMLRequest=.....&SigAlg=.....&Signature=.....>
- Once the user is authenticated, PIDaaS Platform returns to SP the SAML Assertion containing both the Authentication Statement and the Attribute Statement with the required attributes by SP.

Regarding the implementation, SAML Request messages must include the `<samlp:AuthnRequest>` element, which contains the information that identifies the issuer and the receiver (the PIDaaS Platform), among other. In this sense the AssertionConsumerServiceURL, the Destination and the Issuer elements have to be specified with the corresponding URLs. These messages are often carried directly in the URL query string of an HTTP GET request where the `<samlp:AuthnRequest>` element is deflated (sans header and checksum), base64-encoded and URL-encoded, in that order. On the other hand, SAML Response messages are transmitted by PIDaaS using a HTTP POST binding. This

binding defines a mechanism by which SAML protocol messages may be transmitted within the base64-encoded content of an HTML form control. Therefore, these messages are encoded for use with this binding by encoding the XML into a hidden form control within an HTML form. The HTML document must adhere to the XHTML specification. Upon receipt, SP must decode the SAML Response, verify the validity of the **<Response>** message, and parse the **<Subject>** element to get the PIDaaS user authenticated via PIDaaS. Optionally it can also parse the attribute statements containing user attributes.

Ideally, SPs should integrate this functionality in their web sites or applications as a new “login button”. Depending on SP and the PIDaaS environments, any suitable SAML 2.0 library or framework can be used. In Java environments is recommended the use of the OpenSAML library [7]. Thus, users will start the delegated authentication process by clicking that “button”. Finally, remark that each time a user wants to be authenticated using PIDaaS in a new SP, an account association process must be carried out in advance. For a more detailed information about the implementation of the SAML 2.0 standard see the deliverable D4.2.

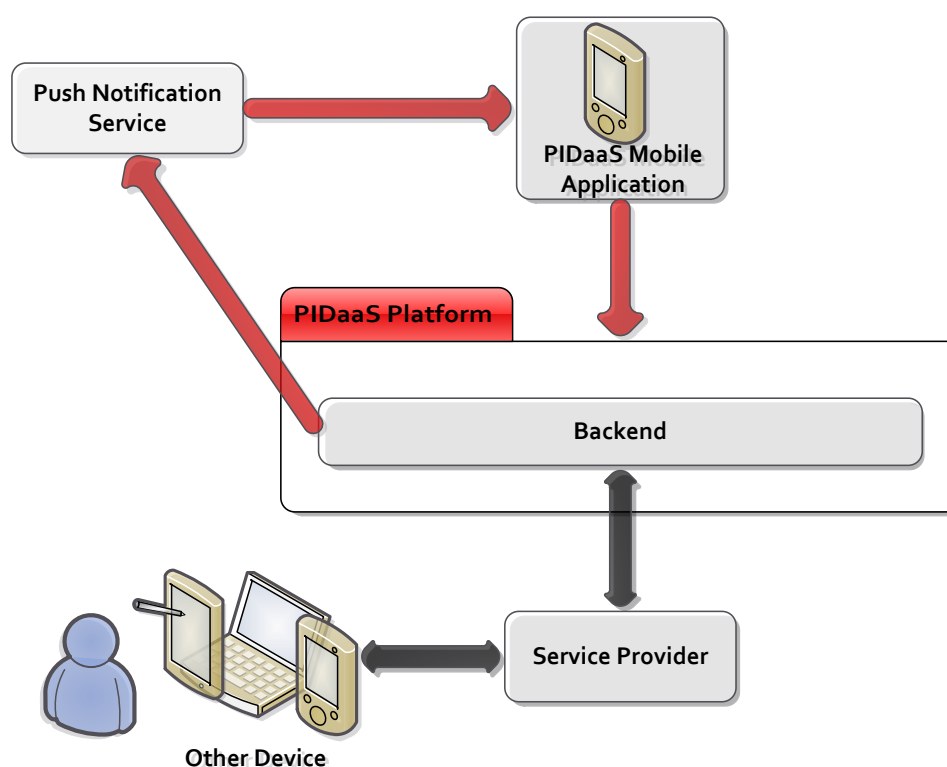


Figure 7. PIDaaS delegated authentication flow

5.1 Association between Service Provider User Accounts and PIDaaS Accounts

Before being able to use the delegated authentication service of PIDaaS, a user needs to associate his SP account with his PIDaaS account. Figure 8 shows the workflow that a user should follow to associate his accounts in a general case.

Next, we describe the process in detail:

Before starting the process, we assume that the user is already logged in PIDaaS with a PMA and in SP (using the account to be associated).

- First of all, **(1) the user clicks the PIDaaS button** to associate the used SAN with his PIDaaS account. Note that this button will be integrated in the “User Area” of SP. Then,
- **(2) the user introduces his PAN** in a form and
- **(3) SP sends the association request with the introduced PAN, the user’s SAN and its SC to PS**, together with other attributes. Once PS has received the request and the related data,
- **(4-5) it checks if the user is logged in PIDaaS** and then it **generates an ephemeral public key D** from the ADs to start the authentication process.
- **(6) PS sends the request authentication as a push notification** to the associated PMA. Note that PS sends the associated seed (sd), D and AT within the push notification.
- Now **(7) the user registers his biometric data**,
- **(8-9) the A-BTPS encoder module generates the public key A and the authentication message M₁** and
- **(10) PMA sends these parameters** together with ST to PS. Next,
- **(11-12) the A-BTPS verification module checks M₁** in order to authenticate the user. If the biometric authentication is successful, the PS starts the process to generate a new biometric template associated to the used SAN. To do so,
- **(13-14) PS sends SC of SP to PMA and the user registers his biometric data (B)**. Then,
- **(15-16) the new ADs is generated in the A-BTPS encoder module** using a certain AT and the user’s B and PAN. Finally,
- **(17) PMA sends to PS the generated ADs**, the associated AT, SC and ST. If all is correct,
- **(18) PS responds SP with an OK**, and
- **(19) SP responds the user with another OK**.

Note that once the process has ended, SP registers the association and PIDaaS stores the tuple (PAN, SC and SAN) in order to univocally identify the association. This process could be done manually by a SP if necessary.

Regarding the integration of this service in a SP, PIDaaS publishes a RESTful API which should be called by SP in order to associate two accounts. This API is protected by the protocol TLS 2.1 in mutual authentication mode using digital certificates and can be only called by a SP previously registered in PIDaaS.

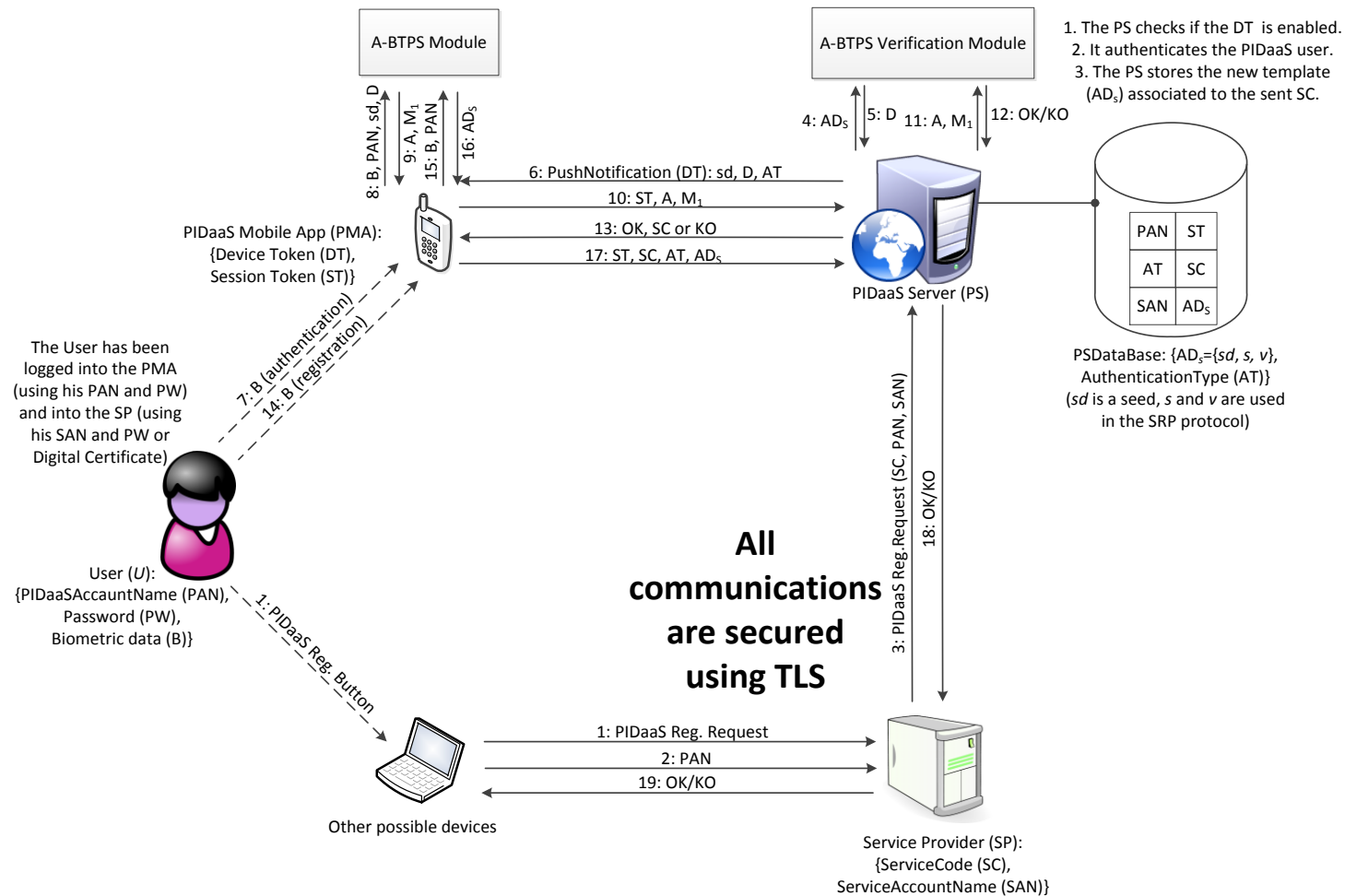


Figure 8: Association process between a PIDaaS account and a SP account

6 Mobile Platforms descriptions

In this section we define the software and hardware requirements of both PIDaaS Mobile App platforms (iOS & Android) to be developed during the 3 pilot phases, software requirements related to PIDaaS Mobile SDK, and also how it is going to be distributed for pilot evaluations.

6.1 PIDaaS Mobile platform HW requirements

Mobile HW requirements for PIDaaS, depends specially on performance required for functionality, and its requirements, to be executed in the Mobile side.

There are not special high-levels requirements for capture processing related to Biometrics systems to be integrated in PIDaaS:

- Image quality during enrollment is important: 640x480 pixels for frontal camera resolution is recommended.
- Good quality microphone also is not required, because functionality to filter out background noises is integrated into the Voice Activity Detection (VAD) module of PIDaaS Mobile SDK.

Finally, these are the minimum recommended HW specifications for using in pilot testing as PIDaaS Mobile device:

- CPU speed: ~ 1-1.5 GHz
- Memory: ~ 1 GB RAM
- Internal Memory: ~ 4-8GB

6.1.1 PIDaaS Mobile iOS HW requirements

Based on the specific iOS requirements related to the graphic design & O.S. version (Mobile App UI is specifically designed for 16:9 aspect/ratio, and functionality programmed for iOS7), our recommendation is as follows:

- Candidate iOS devices for using in pilot testing:
 - iPhone5/5C/5S, 16:9 aspect/ratio device, with iOS7 or higher [iOS8.x]
 - Low: iPhone5 with iOS7 (or higher)
 - Medium: iPhone5C with iOS7 (or higher)
 - High: iPhone5S with iOS7 (or higher)
- Other possible devices for using in pilot testing with same 16:9 aspect/ratio:
 - iPhone6(S) with iOS8.x (or higher)
 - iPhone6(S)+ with iOS8.x (or higher)

- Other possible devices for using in pilot testing, but with different aspect/ratio, therefore not so recommended, are:

iPod Touch (5th generation or higher) with iOS7 (or higher): 71:40 aspect/ratio

iPad with iOS7 (or higher): 4:3 aspect/ratio

iPad Mini with iOS7 (or higher): 4:3 aspect/ratio

iPad Pro with iOS9.x: 4:3 aspect/ratio

6.1.2 PIDaaS Mobile Android HW requirements

Related to Android Platform devices specific requirements, the only requirement is related with its operating system (O.S.):

Android v4.0 (or higher)

6.2 PIDaaS Mobile platform distribution

For the 1st internal pilot, phase 1 (and also probably for phase 2) we will use ‘internal’ distribution³: [TestFairy](#) [8] testing platform. This online tool perfectly meets the requirements of distribution for internal pilots, because is available for both platforms, iOS and Android, but with a limitation of 100 testers per account, that we consider will be enough for the phases 1 and 2 (internal and small scale pilots).

On the other hand, for the large scale pilot distribution, phase 3, because of its limitations, maybe we will have to use other standard official platform tools, as Apple-TestFlight Beta Testing [10] [11] from the Apple Developer Program for iOS platforms & or as Beta Testing for Google Play Apps [12] for Android platforms.

6.2.1 PIDaaS Mobile platform internal distribution: TestFairy

At the TestFairy platform, the app will be uploaded and the participants will be invited to install it on their devices.. TestFairy requires prior registration of the testers devices, before distribution of each Mobile App version, via email, and installation. For more detailed information, you can see the [TestFairy API Documentation](#)[9].

³ However, in case of change/limitation of its conditions, we will look for a similar platform, as well as we did in February 2005, when we decide to use TestFairy, as a real [Apple-TestFlight alternative](#) [10], when Apple decided to acquire and limit the free use of our free candidate iOS testing platform at this time, [TestFlight Beta Testing](#)[11]. Nowadays, this is the current candidate platform for distributing PIDaaS Mobile App Beta versions for IOS platforms in WP5.

You can see below, some PIDaaS real testing snapshots of this process/requirement, Figure 9 to Figure 12:

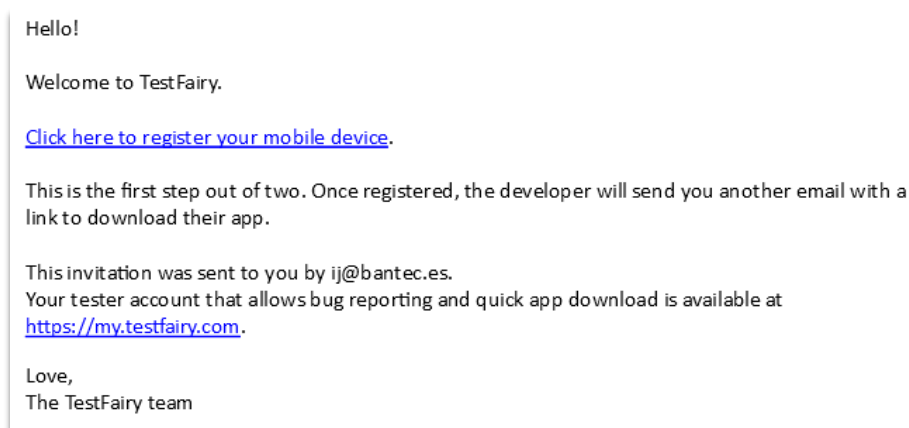


Figure 9: TestFairy Tester Mobile Registration Request email

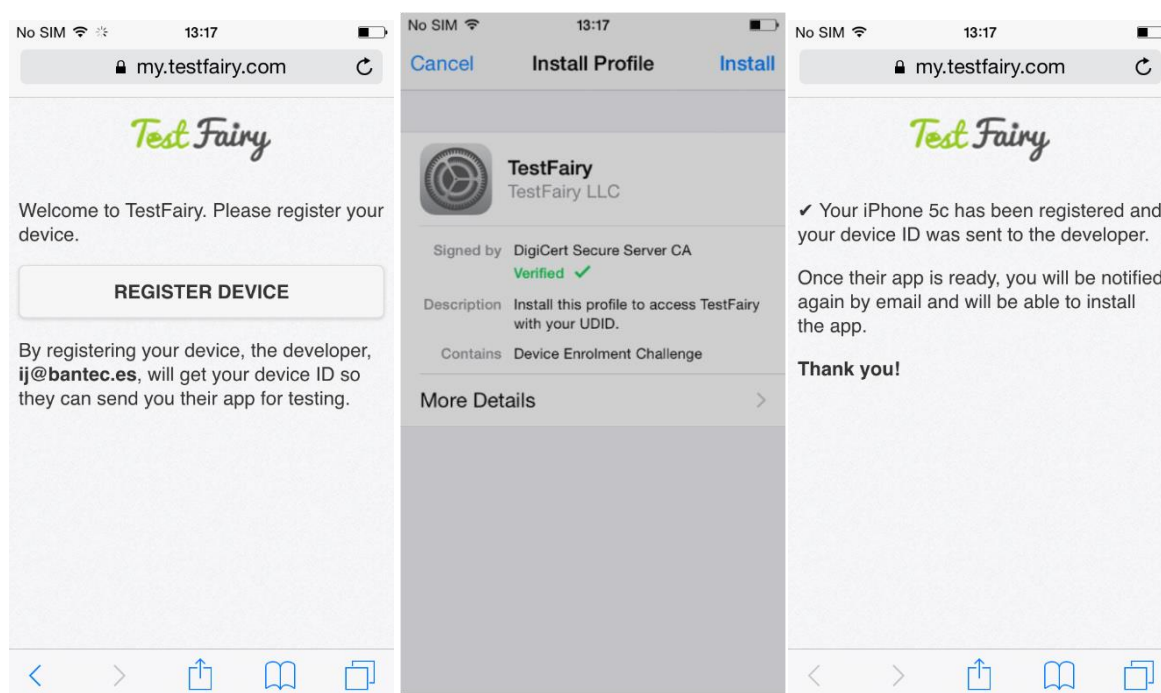
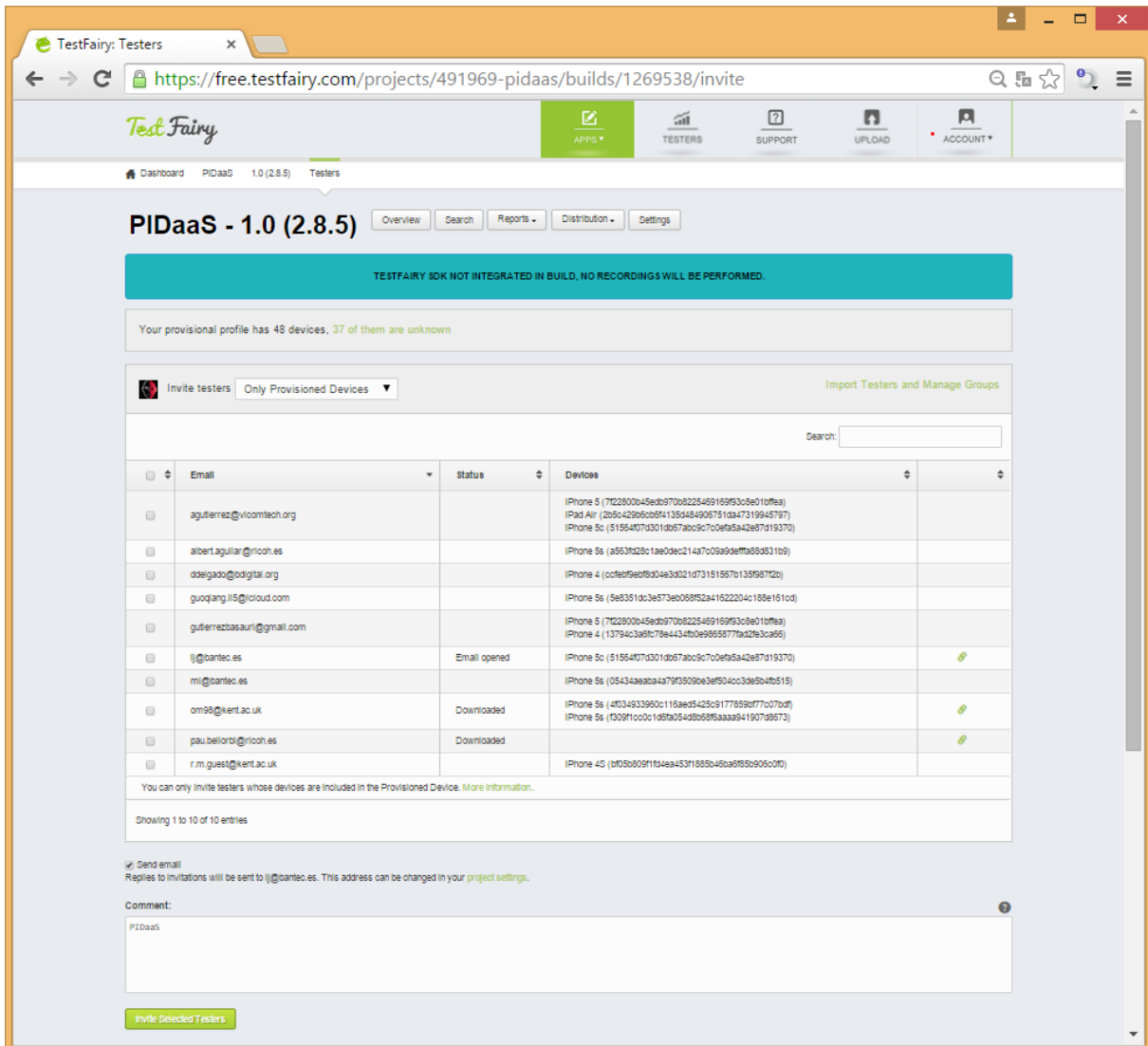


Figure 10: TestFairy Tester Mobile Registration process



PIDaaS - 1.0 (2.8.5) Overview Search Reports Distribution Settings

TESTFAIRY SDK NOT INTEGRATED IN BUILD, NO RECORDINGS WILL BE PERFORMED.

Your provisional profile has 48 devices, 37 of them are unknown

Invite testers Only Provisioned Devices Import Testers and Manage Groups

Search:

Email	Status	Devices
aguiar@vicomtech.org		iPhone 5 (7f22800b45ed970b8225469169f308e10f6a) iPad Air (2b5c42b96c08f413594849057519a47319945797) iPhone 5c (5156407d301db67ab0c9c700efa5a42e87d19370)
albert.aguiar@ricoh.es		iPhone 5s (a553f228c1ae0de214a7009a9deffa88d310b)
ddelgado@odigital.org		iPhone 4 (c0feb95ef80c4e3021d73151567b1359872b)
guoqiang.li@icloud.com		iPhone 5s (5e8351dc3e573e068f52a41622204c188e1610d)
guterrezbasauri@gmail.com		iPhone 5 (7f22800b45ed970b8225469169f308e10f6a) iPhone 4 (13794c3a8c78e4434fb0e985877ba29e3ca96)
l@banteo.es	Email opened	iPhone 5c (5156407d301db67ab0c9c700efa5a42e87d19370)
mi@banteo.es		iPhone 5s (05434aaba94a79f30509e3ef504cc3de5d4b515)
om98@kent.ac.uk	Downloaded	iPhone 5s (4034933960c115aed5425c9177859d77c07bdf) iPhone 5s (f09f1cc0c1d9fb0548b68f5aaa941907d8673)
pau.belloni@ricoh.es	Downloaded	
r.m.guest@kent.ac.uk		iPhone 4S (d05b8091f1d4aa433f1885b48ba9f85e906c0f0)

You can only invite testers whose devices are included in the Provisioned Device. [More information...](#)

Showing 1 to 10 of 10 entries

Send email
Replies to invitations will be sent to l@banteo.es. This address can be changed in your [project settings](#).

Comment:
PIDaaS

Invite Selected Testers

Figure 11: TestFairy web interface Dashboard for Mobile Beta Apps distribution to testers

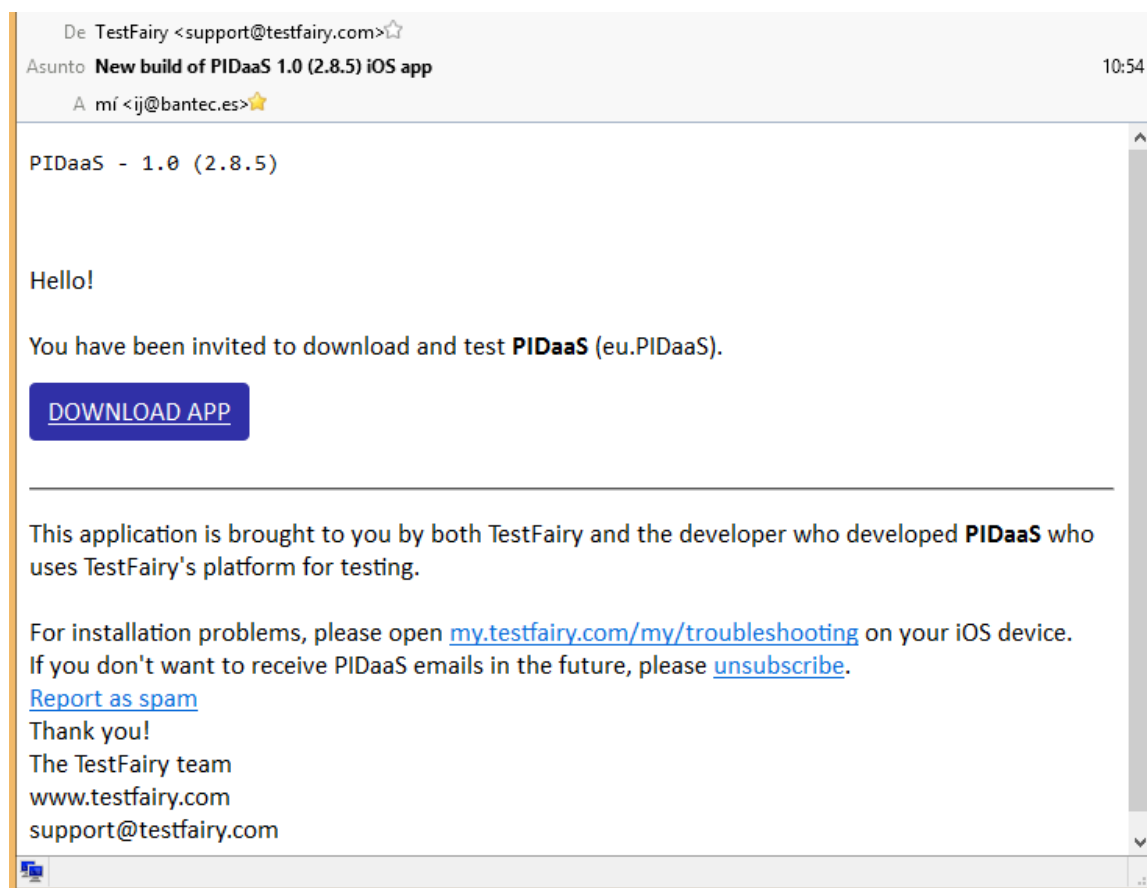


Figure 12: TestFairy Mobile Beta App distribution email to tester

7 Select target population for each phase

In order to smoothly carry out the data collection for pilot at each three PIDaaS Project end-users, we have defined three phases: internal pilot, small scale pilot and large scale pilot. These three phases will target on different participants during the data collection period. The recommendations for selecting those participants for the different three phases are:

- **Phase 1:** as mentioned earlier in Section 4.2, phase 1 is an internal pilot whose goal is to check that all PIDaaS functionalities have been well implemented. Therefore, we recommend at least two persons from the management team to be involved in this phase. The reason of choosing two persons is that they can work individually to make sure all functionalities are working as expected. And they need to understand the background, objectives and the basic knowledge behind the authentication protocol of the PIDaaS project. It is highly recommended that the people who have been working with PIDaaS project since the beginning can be these two persons for this phase. And these two persons will be in charge of the Phase 2 and Phase 3.
- **Phase 2:** this phase is targeting on a small group of participants in order to have a quick response from the people who are not familiar with PIDaaS project before we deploy the PIDaaS to all the end-users' participants. The aim of this phase is to get a quick feedback from those participants. Therefore, we recommend to select these participants from internal employees of our pilot company and those end-users' participants who are frequently using the service from the pilot company. The population of the participants in this phase could be between 15 and 25.
- **Phase 3:** this phase will invite all end-users' participants to use PIDaaS Mobile App for their authentication process when they want to access the service from the service provider.

8 Training material for participants, brief introduction of D4.4

This chapter gives a brief description about the main workflow and procedures of user registration, PIDaaS App login and user authentication from an end-user's perspective by using PIDaaS Mobile App. The details of user registration and authentication procedures will be provided via D4.4 'PIDaaS training material for pilots'.

The participants will need to perform three main tasks:

1. Registration in PIDaaS Platform.
2. Login within PIDaaS App
3. Replay to an authentication request.

8.1 Registration in PIDaaS Platform

During registration process, the user needs to interact with 7 interfaces as shown and explained below. Figure 13 is the start-up page of the registration process where the users need to type their email account (twice in order to verify is correct) which will be used as PIDaaS Account Name.



Figure 13 Start-up page of registration process

Figure 14 illustrates two interfaces: the left one is used to type a PIN (again twice in order to verify is correct) and the right one is to select which biometrics modalities will be used in the PIDaaS Platform. Currently, there are two modalities supported in the PIDaaS Platform: voice and face.

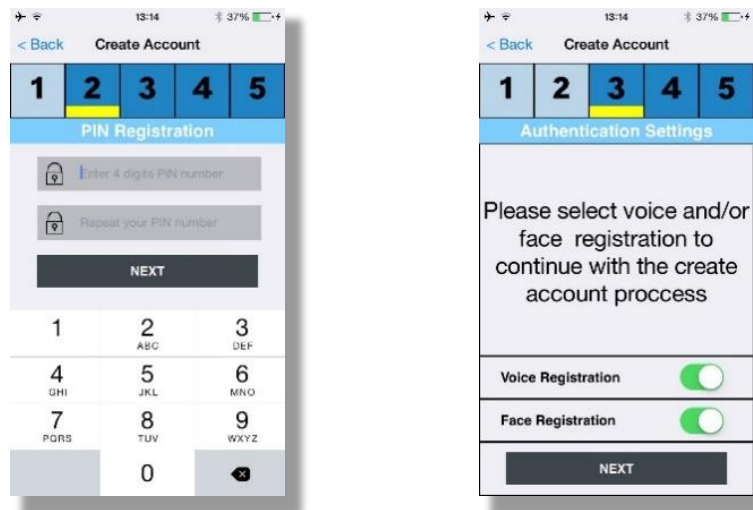


Figure 14 Interfaces for typing PIN and for selecting biometrics modality

After the biometric modality selection, the users need to enrol their voice sample and face image. The voice sample is taken by reading 5 digits displayed by the interfaces shown in Figure 15.

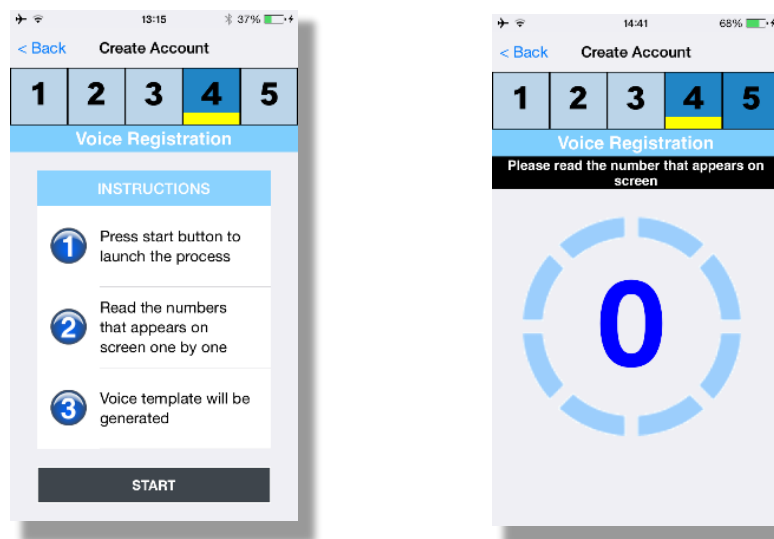


Figure 15 Interface for voice registration

Error! Reference source not found. gives the interface to capture a face sample for enrolment. The users are required to pose properly in order to obtain a good quality face sample and press the capture button.

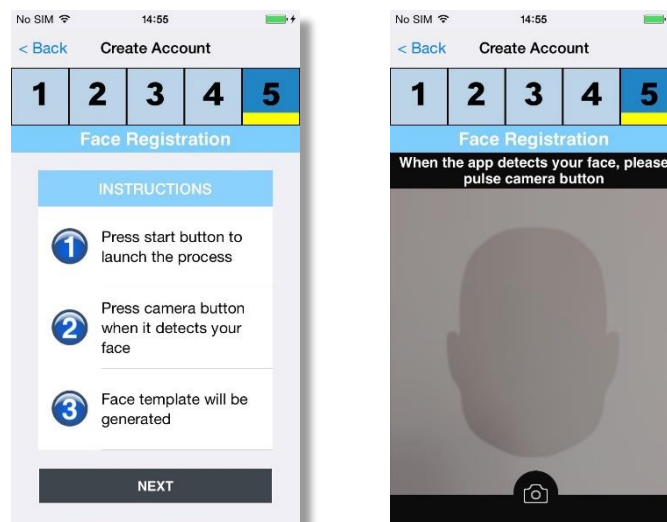


Figure 16: Interfaces for face registration

After the face image enrolment, an ending page will be shown up at the end as seen in Figure 17.

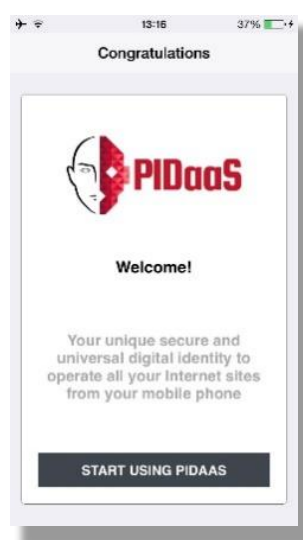


Figure 17 Last page of user registration

8.2 Login in PIDaaS Mobile App

After PIDaaS account registration, the user will be able to login in PIDaaS Mobile App by using his/her biometric information, Figure 18 shows the start-up page of user login where the user should type his/her PIDaaS account name (usually an email address) and PIN.

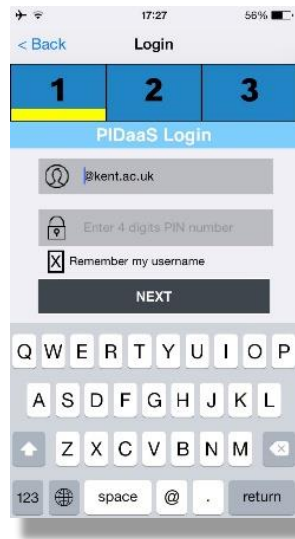


Figure 18 Start-up page of user login

Figure 19 show the interfaces for voice authentication and face authentication respectively.

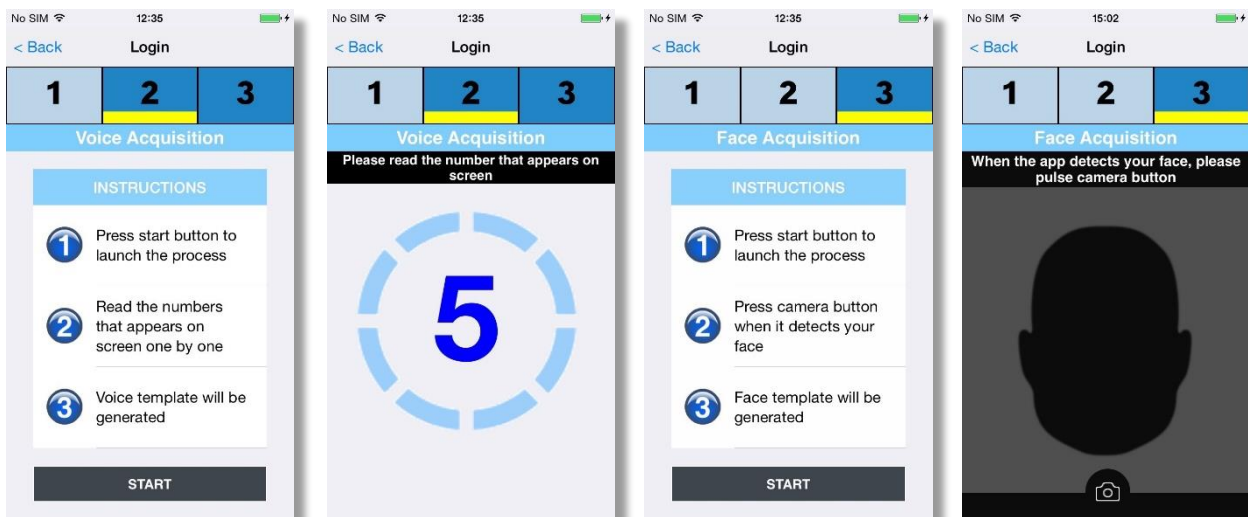


Figure 19 Voice and Face authentication interfaces

If the user successfully completes the login process, the user will be directed to the home tab of the PIDaaS Mobile App, where the user can whether there are pending authentications.

8.3 Replay to an authentication request

If the user's mobile phone receives an authentication request pushed from the PIDaaS Platform, an authentication message will be added to the PIDaaS Mobile App home page as shown in Figure 20:



Figure 20 Authentication request message in PIDaaS Mobile App

If the user selects a specific authentication requests, the user will be prompted to the screen showed in Figure 21, where it can be seen the authentication request details: Service Provider, general information, date and time and description.

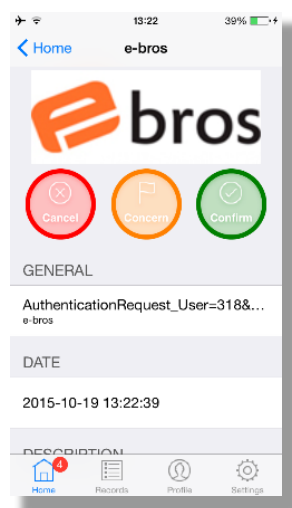


Figure 21 Authentication request details

From this screen the user can perform three different actions:

- **Cancel:** no longer want to perform the authentications.
- **Concern:** inform of a suspicious authentication request.
- **Confirm:** provide your voice and/or face in order to authenticate your identity.

If the user decide to confirm the authentication, the user will process this authentication request providing biometric information. The interfaces used for providing the biometric samples are same as used in login process shown in Figure 19.

9 Usability, privacy and security performance analysis, brief introduction of D4.5

The deliverable D4.5 “Test Plan” document will describes the methodology for the usability, privacy and security evaluation of the PIDaaS Platform that will be performed by the Univesity of Kent (usability evaluation) and the Gjøvik University College (privacy and security evaluations).

This methodology will be applied to the data collected from participants at the WP4 evaluation sites (University of Kent and Gjøvik University College) and the data collected from end-users’ participants in phase 2 and 3 of their pilots.

In this deliverable will be detailed all the log information collected and how this raw data information will be processed and analysed to calculate the different metrics of the usability, privacy and security evaluation. In addition, the usability and security will be analysed for each phase, and corresponding recommendations will also be given to the development partners after each evaluation in order to improve PIDaaS platform and PIDaaS mobile App.

References

- [1] Brockly, M., Elliott, S., Guest, R., & Gonzalo, R. B. (2014). Human-Biometric Sensor Interaction. In S. Z. Li & A. K. Jain (Eds.), Encyclopedia of Biometrics (pp. 1–9). Boston, MA: Springer US. http://doi.org/10.1007/978-3-642-27733-7_2261-3
- [2] ISO 13407:1999, “Human-centred design processes for interactive systems”,
- [3] ISO/IEC 24745:2011, “Information Technology – Security Techniques- Biometric Information Protection”.
- [4] ISO/IEC 2382-37:2012, “Information technology -- Vocabulary -- Part 37: Biometrics”
- [5] Simoens, Koen, Bian Yang, Xuebing Zhou, Filipe Beato, Christoph Busch, Elaine M. Newton, and Bart Preneel. "Criteria towards metrics for benchmarking template protection algorithms." In Biometrics (ICB), 2012 5th IAPR International Conference on, pp. 498-505. IEEE, 2012
- [6] OASIS. Security Assertion Markup Language (SAML) V2.0. <https://wiki.oasis-open.org/security/FrontPage>
- [7] OpenSAML 2: <https://wiki.shibboleth.net/confluence/display/OpenSAML/Home>
- [8] TestFairy: <https://testfairy.com/>
- [9] TestFairy API Documentation: <http://docs.testfairy.com/index.html>
- [10] TestFlight alternative: <http://blog.testfairy.com/testflight-android-alternative/>
- [11] TestFlight Beta Testing: <https://developer.apple.com/testflight/>
- [12] Beta Testing for Google Play Apps: <https://support.google.com/googleplay/android-developer/answer/3131213?hl=en>