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

D2.2
User requirement analysis report
Strategic Positioning report (M7)

Nature[1]: R
Dissemination level[2]: PU
Due date: 31/01/2015
Date of delivery: 31/01/2015

Partners involved:

- CONSORZIO PER IL SISTEMA INFORMATIVO (CSI-PIEMONTE)
- BANTEC CONSULTORES INICIATIVAS EMPRENDEDORAS SL (BANTEC)
- FUNDACIO PRIVADA BARCELONA DIGITAL CENTRE TECNOLOGIC (BDIGITAL)
- RICOH SPAIN IT SERVICES SLU (RICOH)
- FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. IGD (FRAUNHOFER)
- UAB E-BROS (E-BROS)
- FUNDACIO TICSALUT (TICSALUT)
- HOGSKOLEN I GJOVIK (GUC)

[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)

Authors:

Iván Jiménez (BANTEC), Albert Aguilar, Fernando García & Alejandro de Oleza (RICOH), Jesús Berdún & Margarita Hospedales (TICSALUT), Arnau Vives & Juan Caubet (BDIGITAL), Laisvunas Butkus & Linas Eriksonas (E-BROS), Bian Yang (GUC) & Maria Luigia Bosco (CSI-PIEMONTE).

Revision history

Rev.	Date	Partner	Description	Name
1-1.0	03.12.2014	BANTEC	Outline	Iván Jiménez
2-2.0	18.12.2014	RICOH	Section 2 contributions	Albert Aguilar & Alejandro de Oleza
3-2.0	22.12.2014	TICSALUT	Section 3.2.3 contributions	Jesús Berdún
4-2.0	13.01.2014	BANTEC	Section 2 & 2.1 revision	Iván Jiménez
5-2.0	14.01.2014	BDIGITAL	Section 2.3 contributions	Arnau Vives Juan Caubet
6-2.1	16.01.2014	BANTEC	Section 2 & 2.1 contributions	Iván Jiménez
7-2.1	19.01.2014	BDIGITAL	Section 2.4 contributions	Arnau Vives
8-2.2	19.01.2014	E-BROS	Section 4 contributions	Laisvunas Butkus & Linas Eriksonas
9-2.3	21.01.2014	GUC & CSI-PIEMONTE	Section 3 contributions	Bian Yang & Maria Luigia Bosco
10-2.4	27.01.2014	TICSALUT	Section 4 & 5 contributions	Jesús Berdún, Margarita Hospedales
11-2.5	28.01.2014	TICSALUT, RICOH, CSI-PIEMONTE, GUC, E-BROS & BANTEC	Section 5 & Conclusions from Chapters 2, 3 & 4 contributions	Jesús Berdún, Fernando García, Maria Luigia Bosco, Bian Yang, Linas Eriksonas & Iván Jiménez
12-2.6	28.01.2014	BANTEC	Final Formatting & Conclusions	Iván Jiménez
13-2.7	28.01.2014	ALL PARTNERS	Final Review	Iván Jiménez
14-2.8	30.01.2014	E-BROS & TICSALUT	Last contributions	Linas Eriksonas & Jesús Berdún
15-3	30.01.2014	BANTEC	Final Integration	Iván Jiménez

INDEX

FIGURE & TABLE LIST

ACRONYMS LIST

DPM	Direction Policy Matrix
SWOT	Strengths, Weaknesses, Opportunities and Threats
USP	Unique selling proposition
BTP	Biometric Template Protection
BTPS	Biometric Template Protection Scheme
LMP	Life Management Platform
MFA	Multi-Factor Authentication
PIN	Personal Identification Number
SDK	Software Development Kit
DoS	Denial of Service
EHR	Electronic Heath Record
HIPAA	Health Insurance Portability and Accountability Act

1 INTRODUCTION

One of the objectives of WP2 is to define a strategic positioning for the PIDaaS platform in the market. Following the initial market review provided in D2.1, the next step is to decide this strategic positioning PIDaaS platform by analysing possible strategic directions. This is the main objective of this deliverable D2.2 - Strategic positioning report -.

This analysis will be based on the determination of the basic parameters for the identification of the current situation and the future positioning of PIDaaS platform and the selection of proper strategic actions that cover the existing weaknesses and deficiencies. Towards this aim, the direction policy matrix (DPM) will be used, which is a methodological tool for the strategic positioning of a service within the market. But previous to this task, this deliverable also will include an analysis of strengths, weaknesses, opportunities and threats (SWOT Analysis). This SWOT analysis will be based on the results of the initial market review in D2.1, which highlights the competitive advantages, the risk elements and the key priorities that should be taken into consideration during the full deployment of the PIDaaS platform offering.

D2.2 will provide a SWOT Analysis of three main Technologies that compound PIDaaS Platform - Biometric authentication technology, Life Management Platform (LMP) & Biometric Template Protection (BTP) - as well as of the PIDaaS Platform itself, and also taking into account the three targeted markets (e-Commerce, e-Citizen and e-Health).

1.1 Deliverable Objectives

This document includes different analysis in order to identify the most appropriate approach for the strategic positioning of the PIDaaS platform offered to the market. The analysis of possible strategic directions, and identification of strengths, weaknesses, opportunities and threat (SWOT analysis) will be based in the information and conclusions included in previous deliverable D2.1 - Market Analysis report -.

1.2 Summary

This deliverable is structured in different sections, according to the deliverable objectives defined. Below there is a description of the contents in each section.

1. Introduction: Introductory chapter to Deliverable D2.2, including deliverable objectives, summary of contents and methodology.

2. PIDaaS Platform & Technologies SWOT analysis: SWOT Analysis of three key technologies involved in this project (Biometric Authentication Service, Life Management Platform [LMP] & Biometric Template Protection [BTP]).

3. PIDaaS specific markets (e-Commerce, e-Citizen and e-Health) SWOT analysis: SWOT Analysis of the PIDaaS Platform itself, and in specific markets related to the three scenarios to be trialled in the PIDaaS project (e-Commerce, e-Citizen and e-Health).

4. PIDaaS Platform Directional Policy Matrices (DPMs):

4.1. Set of Basic Parameters in different analysis perspectives: Analysis and identification of different sets of basic parameters for the identification of the current situation and the future positioning of PIDaaS platform in different analysis perspectives.

4.2. PIDaaS Platform DPMs related those different analysis perspectives: For each identified set of basic parameters, direction policy matrix (DPM) related to PIDaaS Platform.

5 Conclusions: Final remarks and conclusions about the deliverable, highlighting the competitive advantages, as well as main risk elements and key priorities that should be taken into consideration during the full deployment of PIDaaS platform.

6. References: Citations in the Deliverable.

1.3 Methodology

The methodology followed to develop this deliverable has been based mainly in the following procedures:

For section 2 & 3, SWOT Analysis methodology applied to three key Technologies and to PIDaaS Platform, as well to the specific markets related targeted PIDaaS scenarios.

For section 4, after an identification of different analysis perspectives, Directional Police Matrix (DPM) methodology tool have been used in order for the strategic positioning of a service within the market.

2 PIDAAS PLATFORM & TECHNOLOGIES SWOT ANALYSIS

The objective of this section is to situate and understand the PIDaaS platform and the three technologies integrated (Biometric Authentication Service, Life Management Platform, and Biometric Template Protection) in the market by analyzing the different internal and external factors that can enhance as well as obstruct its development and success. The analysis aims to give an overview of customer expectations, the competition, policies and regulations, and the potential market.

The structure of the document will be defined for the following subsections:

1. 2.1: PIDaaS Platform SWOT Analysis
2. 2.2: Biometric Authentication Service SWOT Analysis
3. 2.3: Life Management Platform (LMP) SWOT Analysis
4. 2.4: Biometric Template Protection (BTP) SWOT Analysis

Elements to consider in the SWOT analysis and results expected are defined in the following:

Internal

Strengths outline the platform characteristics that differentiate and give it an advantage over other existing competitors.

Weaknesses outline the platform characteristics that give a disadvantage. It is important to identify these elements in order to improve the platform.

External

Opportunities identify the factors and elements that the project can exploit/take advantage. It is important to identify these factors in order to increase the probability of success and understand what actions have to be taken to achieve the best possible outcome.

Threats identify the factors and elements that could put the project at risk. These factors are important since they give an understanding of what type of threats can be encountered during the development of the platform. Hence, identifying the actions that can be taken to prevent or diminish the damage.

The following SWOT analysis is based on the results of the initial market review and highlights the competitive advantages, the risk elements, and the key priorities that should be taken into consideration during the full deployment of the PIDaaS platform offering. This analysis will allow defining a successful strategic positioning for the PIDaaS platform.

2.1 PIDaaS Platform SWOT Analysis

2.1.1 Strengths

*Identify the **key strengths** that clearly differentiate the platform technology and give it a major competitive advantage over its competitors.*

- Biometric Data is not exchanged
- Users know whom, when, why their personal data has been used
- Increased security with Biometric Multi-factor Authentication
- Cancelable biometrics
- Easy-to-integrate toolkit, which allows an effortless integration of biometric authentication, identity assurance and user's personal data management within their process
- Users will be able to create securely bioidentities within their mobile devices

- Users will be able to set expiration-dates for the validity of bioidentities as well as immediate cancellation of its use
- Benefits of integrating three technologies vs. different platforms for each technology
- Integration of expertise from developers of the different platform
- Identify the brand recognition of the different technologies
- Resources available from integration
- Unique selling proposition (USP) - product differentiation
- What differentiates each technology
- Effectiveness/precision of each technology
- How do the different technologies complement each other
- Difficulty of replication by competitors
- Reliability with Biometric Multi-factor Authentication

2.1.2 Weaknesses

*Identify the **key weaknesses** that need to be focused on to improve the platform technology.*

- Difficulty of integrating three technologies into one platform
- Changes in privacy laws are unpredictable
- Difficulty to integrate biometric processes into mobile services and application development
- Security preservation of biometric data in the authentication process (need to enroll all the users for each application)
- Lack of user control and privacy issues for an efficient identity management between different applications and domains
- Template capacity that limits amount of information
- Capacity of the system to detect and reject the attempts of authentication on the part of not authorized users as well as to anticipate not identification on the part of users who try not to be recognized

2.1.3 Opportunities

*Identify the **key opportunities** that could play a major role in the growth and development of the platform technology*

- Low competition offering same service
- Identify new trends that support platform development
- Social interest in product
- Potential market growth, people are accumulating more and more personal data and application power in their portable smart devices. This drives a need for more security, and a drive toward personalization
- Slow adoption of technology by competitors
- The incipient offer of similar platforms is finding a good acceptance on the part of companies and end-users
- Implantations representative of similar platforms do not exist in the areas of the markets initially target of the platform PIDaaS.
- Technology can be used/adapted to many different segments (commercial and consumer products, finance industry, healthcare, cyber security)
- Estimated 5,500 million users at 2019
- Gartner estimates in its report that in just two years, in 2016, 30% of companies will have opted for biometric authentication systems on mobile devices to their employees

2.1.4 Threats

*Identify the **key threats** that could challenge the platform technology*

- Changes in privacy laws that could affect platform functionality
- New technologies competing for the same market
- Replication of technology by other companies
- Functionality issues of integrating the three platforms
- Degree of acceptance, disposition of the users to use biometric technology
- Consider the social and cultural factors that can suppose that the technology is more accepted or less accepted depending on the environment where it is implanted

SWOT Analysis remarks - It is necessary to obtain a correct integration of three different technologies included in the platform. Since it is a product that can be developed by other competitors, the PIDaaS platform must be developed in the least possible term and emphasizing the distinguishing values of safety with regard to the possible competition.

2.2 Biometric Authentication Service SWOT Analysis

The objective of this section is to situate and understand Bantec's Biometric Authentication Service platform in the market by analyzing the different internal and external factors that affect its business.

2.2.1 Strengths

*Identify the **key strengths** that clearly differentiate the technology and give it a major competitive advantage over its competitors.*

- Reliable, secure, easy to use
- Reduces the complexity of the authentication process
- Universal user identity service: a single universal identity service for all digital services
- Multi-Factor authentication solution: 2nd factor Biometric Authentication service
- Technology works across computers, smartphones, and tablets and does not require any new hardware
- Precision of authentication service
- Biometrics is regarded as the most fool proof system of identification
- Allows user to create and manage their unique digital identity from their mobile phone completely securely, quickly and simply using voice biometric verification technology
- Exploits the great availability of mobile devices and their capacities for capturing voice biometric samples
- Eliminates the impact of password theft or phishing by supplementing legacy username-and-password logins using unique voice data
- User friendly platform & non-intrusive biometric with high social acceptability
- Security of platform for users
- Required HW low cost in comparison with other Biometric solutions
- Relatively inexpensive compared to other biometrics

2.2.2 Weaknesses

*Identify the **key weaknesses** that need to be focused on to improve the technology.*

- Identify the possibility of platform failure or authentication error

- Few use, at the moment, of the biometric authentication by the general public
- Template capacity
- Identity probability of theft risks
- No Multi-factor policies determined by user location
- No Multi-factor Biometric Authentication: Less Robust in terms of Security
- No randomization in Authentication process
- Processes of data acquisition and data storage represent the main obstacles to this technique
- Gathering accurate voice data is entirely dependent on the quality of capture devices used and thus the absence of noise
- Can be affected by physical condition or emotional state
- Sensitive to differences in microphones used during enrolment and authentication
- Low accuracy & slow in comparison with other Biometric solutions

2.2.3 Opportunities

*Identify the **key opportunities** that could play a major role in the growth and development of the technology*

- Growth potential and development of platform
- Service is being demanded each time more
- More products with types of biometric authentication such as computers and smartphones
- Security concerns growth by consumers results in higher demand for biometric services

2.2.4 Threats

*Identify the **key threats** that could challenge the technology*

- Replication of technology by other companies
- New technologies that could challenge this platform & technology
- Changes in privacy laws that could affect technology
- Reliability (vulnerable to replay attacks)

SWOT Analysis remarks - Biometric authentication is the technology that is part of the PIDaaS platform, which currently has more competition in the market. For this reason, an authentication service that stands out for its ease of use and precision must be achieved.

2.3 Life Management Platform (LMP) SWOT Analysis

The objective of this section is to situate and understand BDigital Life Management Platform in the market by analyzing the different internal and external factors that affect its business.

2.3.1 Strengths

*Identify the **key strengths** that clearly differentiate the technology and give it a major competitive advantage over its competitors.*

- Store and share personal data selectively
  - LMP provides a secure storage of information, becoming something more than a Personal Data Management.
  - LMP provides a secure way to share and process information, adapted for the user needs and desires.

- LMP allows the management of unbounded types of information, like health personal data, car insurance, and so on.
- LMP enables the management of multiple profiles for different types of services, or by user's desire.
- LMP offers integrated management modules of Authentication and Authorization, in order to manage the identity of users and their permissions for the selected services. It even allows the inclusion of third-party authentication.
- Use standardized APIs for privacy and "selective sharing".
- LMP offers a new way to create a trust relationship in a distributed environment.
- LMP is a producer of individual data for other parties, that is, Controlled Push, (i.e. an individual requests access to an online insurance service to buy the car insurance, providing personal information and car details).
- LMP allows the consumption of information from other parties, that is, Informed Pull (i.e. individual issues a request for information to a group of banks to obtain the best offer for a personal loan).

- Protect personal data from being seen by unwanted parties
  - The protection of security and privacy is key and is achieved by the use of severe access controls, among other measures.
  - There are strict policies of Rights and Responsibilities for using personal data, for both users and also service providers.
  - LMP offers a new approach to protect personal information in a decentralized and distributed network.
  - Any request to access to personal data can be restricted by the LMP.

- Control access proactively
  - LMP offers a user-centric management point, giving the user the decision point role of his information.
  - LMP also offers an Accountability module for monitoring, traceability, and audit control.
  - LMP offers a new way to control what is happening to individuals' personal data.
  - LMP offers a new way to help individuals understand how personal data is used.

2.3.2 Weaknesses

*Identify the **key weaknesses** that need to be focused on to improve the technology.*

- There is an Availability issue. LMP can work by itself, but it needs of a widespread use of their users and service providers for really taking advantage of all their potential.
- In order to adopt the LMP platform, (heterogeneous) service providers are required to integrate with the LMP. As every service provider could be using different technology, even different devices (e.g. PC, mobile phone, tablet, etc.), LMP shall offer integration modules covering the broadest type of technologies.
- A Denial of Service (DoS) attack, or a failure of the system of LMP, could affect all services which are consuming information from the platform, so it creates a dependency of the services.

2.3.3 Opportunities

*Identify the **key opportunities** that could play a major role in the growth and development of the technology*

- A high percentage of users demand an identity management platform in order to ease their life (not to remember passwords anymore, auto-fill registration forms, manage their custom policy measures, obtain relevant data according to their selected needs/profile, etc.).
- Service providers demand a platform which manages the authentication and authorization, simplifying their requirements.
- Service providers demand a platform which could refine their offers that could be made to a more precise user profile.
- To protect privacy and confidentiality among the service providers is a challenge (need to fulfill law directives), but in fact it raises the opportunity to become a relevant platform useful for both users and service providers.
- With this platform, it becomes an opportunity for consumers to get more up-to-date information, as identity is managed in a single point.
- Users can quantify their shared data across the multiple services, in order to "monetize" their profile.
- LMP can provide an alternative to the current "terms and conditions" paradigm. These contracts allow big companies to use information about users to do their business.

2.3.4 Threats

*Identify the **key threats** that could challenge the technology*

- Difficulties in the integration with service providers could be met (e.g. friction with technologies used by service providers, etc.).
- Reluctance of either users or service providers to adopt this platform becomes of high importance.
- Fulfillment of legal constraints (privacy) in each type of service provider could be more complicated than expected, as could be changing in time, and adaptation shall be done for each country.
- Too many features could disorientate users. The solution needs to be concise, clear, and easily manageable.
- LMP is a trust-based system. Once data is requested from consumers and is given to them, that piece of shared information is fully controlled by the consumers, and could be even shared to third parties. This can be useful if assessed correctly, but could be a threat in case of misbehavior.
- LMP is a clear target for hackers, as sensitive information about its users is centralized. So the protection of the security and privacy of users becomes key and could be a threat if compromised.

SWOT Analysis remarks - Because it is necessary for service providers to adopt the platform LMP, it is necessary to obtain a development of the technology that stands out with respect to the competitors, especially in safety terms and usability.

2.4 Biometric Template Protection (BTP) SWOT Analysis

The objective of this section is to situate and understand Fraunhofer-IGD Biometric Template Protection platform in the market by analyzing the different internal and external factors that affect its business.

2.4.1 Strengths

*Identify the **key strengths** that clearly differentiate the technology and give it a major competitive advantage over its competitors.*

- Biometric template protection scheme can be applied to any biometric features whose binarizations are uniformly distributed for different users and show little variation for the same user
- Enables anonymous biometric templates (multiple templates for one user, from one-way template cannot recover the biometric sample)
- Cancelable biometrics
- Full automation
- Define security levels compared to competitors
- World's leading institute for applied research in Visual Computing
- Speech spectrum has shown to be very effective for speaker recognition

2.4.2 Weaknesses

*Identify the **key weaknesses** that need to be focused on to improve the technology.*

- Identify the possibility of platform failure or information storage error
- Verification and storage in the 'cloud', not in local storage
- User reluctance on privacy issues, consumer trust

2.4.3 Opportunities

*Identify the **key opportunities** that could play a major role in the growth and development of the technology*

- Privacy-enhancing biometric templates can become of great acceptance for users
- Identify competitors, their market share and success/difficulties encountering
- Competitive advantage

2.4.4 Threats

*Identify the **key threats** that could challenge the technology*

- Identify cyber threats and vulnerability of platform
- Identify the possibility of new technologies that could enter the market
- Changes in privacy laws that could interfere with platform

SWOT Analysis remarks - It is necessary to emphasize the development of the BTP technology in obtaining the biggest possible safety of the information, as well as the minimization of possible mistakes or errors in the storage of the information. These safety values will have to be transmitted to the potential markets.

3 PIDAAS SPECIFIC MARKETS SWOT ANALYSIS

Utilising the results of previous Section 2, PIDaaS specific markets SWOT analysis was assessed. These markets are related to the three scenarios to be trialled in the PIDaaS project (e-Commerce, e-Citizen and e-Health).

3.1 e-Commerce market SWOT analysis

3.1.1 Strengths

*Identify the **key strengths** that clearly differentiate the market technology and give it a major competitive advantage over its competitors.*

- Addressing threats of biometric identity theft by storing only converted data – no raw data to be stored
- Providing users with a tool for managing own identity via integrated life management system
- Simplifying access to constantly used secured sites (including e-commerce) avoiding need to use multiple user names and passwords
- Cloud based solution which makes implementation for e-commerce solution providers and e-commerce operators technically easier
- Cloud based solution which allows to minimize infrastructure investment
- Avoiding possibility that customers are sharing their access identities to third parties, this way allowing third parties to access e-commerce using customer logins. It is actual in competitive B2B environment where customer might pass over own credentials to competitor of e-commerce site operator (illegal praxis) this way making confidential info available to competitors
- Multi-mode biometrics which is used in single system (voice and face) to achieve higher security or better convenience

3.1.2 Weaknesses

*Identify the **key weaknesses** that need to be focused on to improve the market technology.*

- Possibility of unacceptable fail-to-enroll and fail-to-extract rate in uncontrolled environment (noisy, dark environment) to generate a biometric template
- Need of developing and supporting system for multi-platform environment as only this way operators of e-commerce will be sure they don't lose customers who use non-supported mobile device

3.1.3 Opportunities

*Identify the **key opportunities** that could play a major role in the growth and development of the market technology*

- Increasing concern about security is supporting search for reliable authentication methods by e-service providers
- Privacy concern over biometrics can be alleviated by BTPS.
- Already wide and constantly increasing usage of smart mobile devices makes PIDaaS solution easily available for majority of population without extra investment into any special devices

3.1.4 Threats

*Identify the **key threats** that could challenge the market technology*

- Need to educate both end users and e-commerce system providers and operators about biometric authentication benefits in terms of security, usability etc.
- Market inertia and as a consequence slow adoption rate
- E-commerce solution providers and operators might see no commercial value of deploying biometric authentication system and bearing related costs
- Necessity to create sufficient number of e-service providers implementing PIDaaS as end customer would start to feel a value in joining PIDaaS authentication service
- Potentially not fully harmonized legal environment related to biometric data in EU or world-wide could make global roll-out harder

SWOT Analysis remarks – while PIDaaS might be able to provide e-Commerce users a secure and privacy-preserving way to authenticate themselves without need of forwarding their identities to third parties, PIDaaS needs both a well-built platform which is interoperable with different computing environment and mobile terminals, and a good security-convenience trade-off for users.

3.2 e-Citizen market SWOT analysis

3.2.1 Strengths

*Identify the **key strengths** that clearly differentiate the market technology and give it a major competitive advantage over its competitors.*

- Unlike credentials (documents and PIN), biometric traits (e.g., fingerprint, face, and iris) cannot be lost, stolen, or easily forged; they are also considered to be persistent and unique and thus provide trust binding between the citizen to the credential in e-citizen services.
- Use of biometrics is not new; fingerprints have been successfully used for over one hundred years in law enforcement and forensics to identify and apprehend criminals. Thus biometrics should be acceptable for e-citizen use.
- This pilot brings innovation and ease of use in a customary action by the user and thus is useful to access to personal information in e-citizen applications.

3.2.2 Weaknesses

*Identify the **key weaknesses** that need to be focused on to improve the market technology.*

- Mobile phones and tablets is easily lost, stolen or misplaced. These devices are not yet equipped with trusted operating systems and computing environment for e-citizen uses on high trust levels.

3.2.3 Opportunities

*Identify the **key opportunities** that could play a major role in the growth and development of the market technology*

- Prevailing methods of human identification based on credentials (identification documents and PIN) are not able to meet the growing demands for stringent security in applications such as national ID cards, border crossings, government benefits, and access control.
- From the point of view of the credentials, the appropriate level of safety, respecting the principles of proportionality and purpose (§ 4.2.2 in doc "Market analysis report"), allows the use of biometric credentials as required for the pilot project PIDaaS.
- Biometrics Research Group projects that over 90 million smartphones with biometric technology will be shipped in 2014.
- Due to the large number of new smartphones expected to ship in 2014, it is expected that the smartphone mass market will drive rapid growth in consumer electronics biometrics.
- The forecasted spike in popularity will be brought on by the fact that wearable technology offers great potential to support biometric technology for authentication purposes.
- Goode Intelligence has forecast that by 2019 there will be 5.5 billion users of mobile and wearable biometric technology around the globe. Apple is currently the leading manufacturer of biometric enabled mobile and wearable devices.
- The security leaders manage users' expectations when evaluate biometric authentication methods where higher-assurance authentication is required, and take into account the user experience without compromising security.
- Goode Intelligence has also projected that 619 million people will be using biometrics on mobile devices by the end of 2015. Goode also predicts that by 2017, there will be more than 990 million mobile devices with fingerprint sensors.
- The lower cost and improved convenience of these approaches are steadily driving increased adoption.
- PIDaaS is the main EU Project directly addressing integration of this type of technologies without other project as a competitor

3.2.4 Threats

*Identify the **key threats** that could challenge the market technology*

- Gartner predicts that by 2016, 30 percent of organizations will use biometric authentication on mobile devices, up from five percent today: the project could be late. For e-citizen use, products need substantive testing. The 2016 is very close, our project will have produced only prototypes
- What will be truly transformational about the use of biometrics on wearable devices, is the birth of the universal authenticator – a device that intuitively knows who we are, where we are, what we want to do and can open doors – both physical and virtual.
- In 2006, Microsoft had released a fingerprint scanner device to allow users to access its operating system without a password, while in 2012 Google released a facial recognition feature to allow users to access their Android-based smartphones. While both of these technologies are rudimentary and have been subjected to security breaches. For e-citizen use of PIDaaS product, similar security concern may arise from the users.

SWOT Analysis remarks - Biometric technologies of mobile tools are rapidly spreading. The PIDaaS project has long development time and provides a diffusion prototype limited on the country in which the prototype is developed. To avoid the risk of remaining a niche project overtaken by national solutions, as highlighted in section "threats", it could be useful to provide an initial distribution of the prototype in each participating country. The fast and widespread use can lead to involvement on the work tables for the new legislation.

3.3 e-Health market SWOT analysis

3.3.1 Strength

*Identify the **key strengths** that clearly differentiate the market technology and give it a major competitive advantage over its competitors.*

- In hospital management, integration of administrative processes helps to reduce time and effort from both administrative staff and the patient. PIDaaS offer a single platform to manage patient and health staff personal traits, as well as authentication when accessing Electronic Heath Records (EHRs).
- PIDaaS provides tools to capture biometrics directly from mobile devices, thus minimizing implementation cost for authentication methods.
- In PIDaaS platform, no biometric raw data is stored. Personal traits are converted through different templates, thus protecting personal data in case of theft of devices.
- Simplification of access to EHRs and other personal health-related data. Biometric authentication prevents users from having to memorize different logins and passwords.
- Security increase in access control and management through an integrated platform. Access to records by health professionals can be monitored to prevent non-authorized access.

3.3.2 Weaknesses

*Identify the **key weaknesses** that need to be focused on to improve the market technology.*

- PIDaaS needs to meet technical requirements related to integration with Hospital Information Systems and other health-related infrastructures.
- For the application and integration of PIDaaS solution, there is a need to specifically address different legal requirements, according to each country's legislation in the e-Health domain.

3.3.3 Opportunities

*Identify the **key opportunities** that could play a major role in the growth and development of the market technology*

- Increasing consolidation in the global biometrics market addressed to healthcare industry. The analysts forecast the Global Biometrics market in the Healthcare industry to grow at a CAGR of 31.95% over the period 2013-2018 [1].
- Current shift towards patient-centred healthcare services, from provider-based control of medical histories to patient-based control. This is made possible by the patient's own personal security keys based on their biometrics [2].

- Sharing data among health providers require a secured central repository and access control mechanisms, and the combination of biometrics technology and mobile devices provide a ubiquitous healthcare solution.
- Protecting privacy and confidentiality of health records is a current challenge faced by modern health information systems. International regulations such as the imposed by the European Data protection Directive and the HIPAA (Health Insurance Portability and Accountability Act) require high level for access, administration and exchange of medical sensitive data.
- Biometrics is recommended by HIPAA as an approved method of providing entity authentication. Given that, this definition of suitable policies, together with economic reforms, are driving the rapid compression of technology adoption cycles within the healthcare industry [3].

3.3.4 Threats

*Identify the **key threats** that could challenge the market technology*

- Some institutions may be reluctant to interact with platforms such as PIDaaS, due to the legal constraints which affect the deployment of such systems. Lack of awareness or inexperience with biometric systems may hinder the adoption of PIDaaS by public authorities.
- Medical devices and e-Health new technologies are increasingly close and sometimes is difficult to know where the frontier is and thus whether one software, sensor or other e-Health product or device, in addition to fulfilling rules concerning data protection, should also to obtain the CE marking.
- More concern is given to the processing and exchange of health data among health providers, emphasizing the importance of stakeholder's knowledge about legal requirements related to personal health data and other critical information gathered by wearable technology, which may be considered as medical devices.
- User acceptability. Biometric data collected in the e-Health context may be considered too private for some users to be shared. Given that, strong focus should be placed to ensure security and privacy concerns.

SWOT Analysis remarks - Based on the analysis provided in this SWOT analysis, it is essential to focus on developing a user-friendly platform, easy to deploy in terms of infrastructure, with capacity to integrate different services and to secure personal data. Moreover, current trends in healthcare market can facilitate the introduction of PIDaaS solution, given the positive perception of biometrics methods for authentication processes. However, special attention should be addressed to meet local rules and regulations related to privacy, as well as international certifications. Also, efforts should focus on raising awareness about the benefits of biometric technologies, and increasing user acceptability, by providing a multi-platform solution, in order to reach the largest number of end-users.

The aim of this section is to obtain a description of the current state of the market for the technologies involved in the PIDaaS project and for the PIDaaS Platform itself and contribute with strategic considerations for the planned exploitation of the PIDaaS outcomes.

4.1 Set of Basic Parameters in different analysis perspectives

Guidelines for task completion

For the completion of task 4.2 the following procedure (**Figure 1**) was adopted on the basis of the customer profiling methodology provided by the Chartered Institute of Marketing [4]:

1. Identification of potential customer groups and their profiles
2. Preparation of Directional Policy Matrices for the application of PIDaaS product in three specific target markets (e-Commerce, e-Citizen, e-Health)
3. Preparation of consolidated DPMs and recommendations for strategic positioning

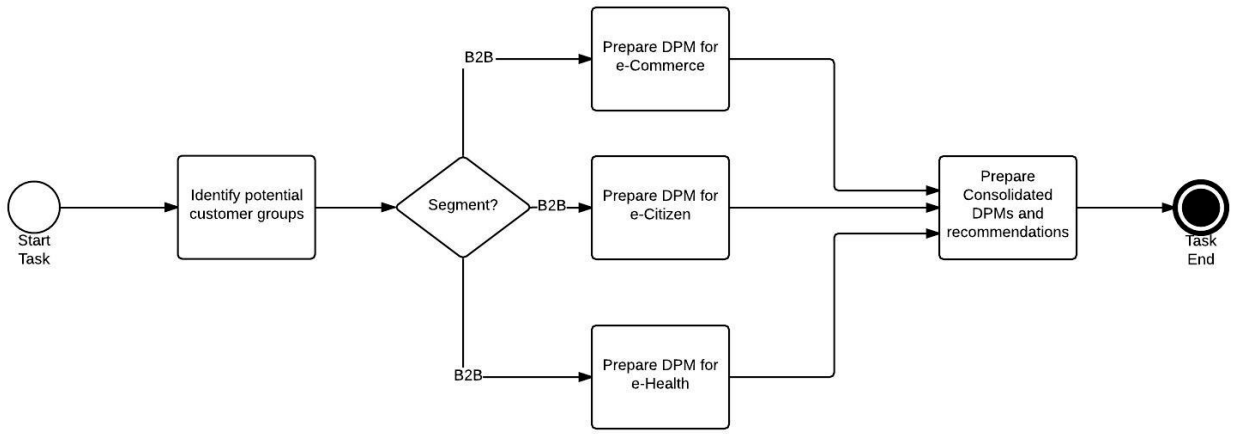

Figure 1: Identification of potential customer groups and their profiles

Potential customer groups have been identified using the following steps:

- Step 1 – Identification which customers are profitable
- Step 2 – Customer profiling
- Step 3 – Definition of customer groups
- Step 4 – Selecting customer groups that will be targeted
- Step 5 – Compiling a target list of prospective customers

Step 1. *Identification which customers are profitable*. By using 80/20 rule we presume that the customers which command 80% of the specific market are the key on whom we should focus most of our efforts. The details about these potential customers in the markets of PIDaaS consortium have been with the help of the partner input.

Step 2. *Customer profiling*. Identification of customer profiles was carried out by asking the expert panel represented by the task group to characterize the top performing customer groups according to:

- The use of existing multi-factor identification systems
- The frequency of the use of those systems
- Particular benefits/functionalities that are need for the PIDaaS type of system to deliver
- Additional "soft" factors that can make PIDaaS products appealing to them

Additional information have been gathered to better understand why individual customer groups buy multi-factor identification systems, who is a typical decision making unit for making those purchasing decisions and why they buy from the existing suppliers.

The following customer profiles have been preliminary identified:

- Profile 1. System Integrators looking for additional SDKs to increase security and thus expanding the existing complexity of their systems and in need to expand their offering of multi-factor authentication systems
- Profile 2. System Integrators looking for decrease of the complexity of their systems and in need to substitute partially their existing multi-factor authentication system with biometric components
- Profile 3. System Integrators re-segmenting market through development of a web front-end and in need to enter IOS or Android app ecosystems through a novel authentication via a mobile phone

Step 3. *Definition of customer groups*. The identified customer profiles (Table 1) have been grouped into customer groupings for potential business according to the most dominant technologies used in multi-factor authentication systems.

Customer profiles/Technologies	*1) Fingerprint recognition*	*2) Face recognition*	*Iris recognition*	*If other*, indicate*
A) System integrators expanding the system complexity	Customer group A1	Customer group A2	Customer group A3	Customer group A4
B) System integrators decreasing the system complexity	Customer group B1	Customer group B2	Customer group B3	Customer group B4
C) System integrators creating novel systems for an app ecosystem	Customer group C1	Customer group C2	Customer group C3	Customer group C4

* - Speaker recognition, Dynamic Signature, Keystroke Dynamics, Retina recognition, Facial Thermography

Table 1: Customer Profiling Methodology - Step 3: Definition of customer groups

Step 4. *Selecting customer groups that will be targeted*. In order to select customer groups out of the identified potential 12 customer groups (Table 1) the ranking has been accomplished using the business objectives (i.e. achieving the largest possible revenue growth with lesser efforts by adopting PIDaaS system) and scoring each group against them using a simple scoring

system 1-3, where 3 is the most attractive. Three groups were identified as best meeting the potential, namely:

1. Target customer group – "SDK buyers for existing systems". System integrators decreasing the system complexity and looking for possibilities to substitute several types of authentication such as dynamic signature and keystroke dynamics (B4)
2. Target customer group – "SDK buyers for mobile front-end applications". System integrators developing solutions for a hybrid or a fully mobile use (C4)
3. Target customer group – "Large system developers". System integrators looking for additional SDKs to increase security

Objective	*A1*	*A2*	*A3*	*A4*	*B1*	*B2*	*B3*	*B4*	*C1*	*C2*	*C3*	*C4*
Few competitors	1	1	2	2	2	2	**3**	2	1	1	**3**	**3**
Potential for better margins	1	1	2	1	2	2	1	**3**	1	1	2	2
Growth potential	1	1	2	2	1	1	1	2	2	2	2	**3**
Mainly large organisations	2	2	**3**	**3**	1	1	2	**3**	2	2	2	1
Total score	5	5	**9**	**8**	6	6	7	**10**	6	6	7	**9**

Table 2: Customer Profiling Methodology - Step 4: Selecting customer groups that will be targeted

Step 5. Compiling a target list of prospective customers

With the help of project partners a list of prospective customers (corresponding to the selected customer group descriptions) have been identified in each country/region of the PIDaaS consortium according to three major segments (as indicated in the table below).

The analysis has identified the following types of customers according to individual segments (as indicated in the table below):

- *Customer Type 1*: A B2C operator of e-retail shops developing in-house solutions and in need to decrease the complexity of the system while increasing additional benefits for the end-users (subcontracting the system development);
- *Customer Type 2*: A B2C operator of e-retail shops looking for additional add-ons for m-commerce (developed internally);
- *Customer Type 3*: A governmental organisation in charge the implementation of digital agenda maintaining IT department and developing applications based on the stored data;
- *Customer Type 4*: A system integrator decreasing the system complexity and looking for possibilities to substitute several types of authentication for e-Health applications;
- *Customer Type 5*: A company developing and implementing complex systems for health sector and requiring multi-factor authentication solutions.

Customer groups / market segments	*E-Commerce*	*E-Citizen*	*E-Health*
SDK buyers for existing systems	e.g. Privalia (end-user, Spain) *Customer Type 1*	e.g. Government of Catalonia (Spain),or Registru centras (end-user, Lithuania) *Customer Type 3*	e.g. Adeslas and FirmaProfesional (Spain) *Customer Type 4*
SDK buyers for mobile front-end applications	e.g. pigu.lt (Lithuania) *Customer Type 2*	No potential customers identified to match this customer profile	Some companies identified to match this customer profile but no conclusive understanding reached whether they form a distinctive customer group (e.g., Doctoralia, Sanitas in Spain, Fitbit and similar mobile health start-ups in the US)
Complex authentication system developers	No potential customers identified to match this customer profile	No potential customers identified to match this customer profile	e.g. BAIP (Lithuania) *Customer Type 5*

Table 3: Customer Profiling Methodology - Step 5: Compiling a target list of prospective customers

In order to better understand the strategic considerations of potential customers and identify tactics for addressing those by offering the PIDaaS solution, the following ten companies were identified as representing "typical" customers each falling under one of five customer profiles:

1. *Privalia (www.privalia.com)*, an online-fashion outlet with operations across Spain, Italy, Germany, Brazil and Mexico, which holds the leading market share in all these markets (the revenue is 422 EUR million). The company is based in Barcelona and might be accessible through the Spanish partners in the PIDaaS consortium. This type of customer is mostly concerned with the issue of how to decrease complexity of the existing electronic payment systems (making them convenient to the customer to use), while increasing security.
2. *Government of Catalonia (www.catalangovernment.eu)* is the main authority in charge of e-citizen agenda is keen on being a leader in Europe in terms of digitalization and increased citizen participation in decision making processes. This type of customer is looking for ready-made solutions to increase security features of the existing authentication systems while making those systems as open and transparent as possible.
3. *Registru centras (www.registrucentras.lt)* is the main public authority responsible for data storage and maintenance of three main state registers, including Real Property Register and Cadastre, the Register of Legal Entities, and the Address Register. In addition it has a function of setting up an e-health register. This type of customer is in

need of opening public data infrastructure to third parties while adhering to a very strict data protection.

4. *Adeslas (https://www.segurcaixaadeslas.es)* is a health insurance company which is a typical customer in need for IT solutions that could ensure the privacy of its clients and create opportunities for patients to get hold of their personal e-health records and use for ensuring a more flexible insurance arrangement based on one's personal needs.
5. *FirmaProfessional (www.firmaprofesional.com)* is a company developing and integrating digital certificate authentication systems for large institutions and companies, some of them in the healthcare sector. This type of customer is in need of extending their current portfolio of offered functionalities, in order to include biometrics multi-factor authentication, so that they could capture a wider scope of requirements and better cater towards individual needs of their customers.
6. *Pigu.lt (www.pigu.lt)* is the largest e-commerce and m-commerce operator in Lithuania - similar companies exist in each national market -. Their need is to increase the customer retention rates on their mobile retail platforms developed internally with the help of open source frameworks. Their need is both simplify the authorization and increase the sense of security among users of m-commerce.
7. *Doctoralia (www.doctoralia.com)* is a global platform for doctor's appointment. Doctoralia healthcare platform connects millions of users with their local medical services. The company's office for Europe is based in Barcelona. The booking system is operated with a mobile front-end. The need of such customer is to provide privacy-conscious customers with additional layer of authentication which could gain on importance for the main customer segment also if e-health data are start to be shared through such platforms.
8. *Sanitas (www.sanitas.es)* is a medical insurance company assisting expats throughout the world to obtain medical health insurance cover in Spain and abroad. The company uses a mobile platform as its main interface serving the customers. Their need is to provide a better access to people who might suffer from injuries and are not able to login physically; hence, the need for multi-factor authentication based on face and/or voice recognition.
9. *Fitbit (www.fitbit.com)* is a retailer of fitness and health-related gadgets. This customer is in constant need of expanding its line of products with items of different functionality. In order to safeguard the personal health and fitness data stored on those devices a need for a hands-free authentication solution could be needed.
10. *BAIP (www.baip.lt)* is a company developing IT solutions for governmental sector and large organisations based on a complex software architecture, including IT infrastructure design, resilience and business continuity assurance, cloud computing, data migration. This type of customer needs to provide multiple layers of authentication in a complex system encompassing both back-end and front-end applications at enterprise computing and cloud computing levels.

4.2 PIDaaS Platform DPMs related those different analysis perspectives

Preparation of DPM for each customer group

DPMs were prepared according to the following procedure. Each expert (representing project partners in the task force of five experts) was given a task to survey at least 2 prospective

customers confirming to the identified customer groups asking them to complete the DPM input table. Altogether 10 prospective customers (as listed above) have been surveyed and their aggregated values have been entered into the cumulative DPM. Two factors were measured – Market Attractiveness and Product Capability.

Market attractiveness was estimated using the following list of criteria (Attractiveness Factors):

- Size of the segment
- Growth rate of the segment
- Profit margins of the segment
- Ongoing purchasing power of the segment
- Attainable market share
- Required market share to break even

Product Capability was estimated using the following list of criteria (Capability Factors):

- Competitive capability of the organisation
- Access to distribution channels
- Capital and human resource investment required to serve the segment
- Brand association of the organisation in the eyes of the segment
- Current market share/likely future market share

The scoring was accomplished as follows:

- Weighting the relative importance of each factor of attractiveness and PIDaaS system capability in terms of its contribution to the goal of the customer group strategy out of 1.
- Allocating the respective weight of a total score of 48 points to each factor. e.g. if the weighting for a factor was 0,2 then the total points available for that factor is 0,2X48=10 (rounded up)
- Scoring each segment relative to the other segments in how much each segment meets the criteria of the factor. E.g. for the attractiveness factor ‘Size of segment’, score the largest segment 10 and the smallest segment 1.
- Plotting the resultant score in excel and creating a bubble chart graph where the size of the bubble represents the size of the segment for greater visual clarity when it comes to interpreting the analysis.

The following weights were used for Attractiveness Factors:

- Size of the segment - 0,2
- Growth rate of the segment - 0,3
- Profit margins of the segment - 0,1
- Ongoing purchasing power of the segment - 0,1
- Attainable market share - 0,2
- Required market share to break even - 0,1

A "growth rate" is considered as the most weighted factor (0,3) given the growth perspectives in biometrics market in healthcare. Size of segment and attainable market share are the following factors considered. Regarding the score, attainable market share scores higher than other factors in this segment, given the potential clients that could be reached in healthcare systems security, given the experience of the company in other security procedures, such as a digital handwritten

signature. Growth rate is also considered relevant, taken into account the tendency to adopt security measures in patient information access.

The following weights were used for Capability Factors:

- Competitive capability of the organisation - 0,2
- Access to distribution channels - 0,3
- Capital and human resource investment required to serve the segment - 0,1
- Brand association of the organisation in the eyes of the segment - 0,3
- Current market share/likely future market share - 0,1

Access to distribution channels and brand association of the organization are considered to have more weight than the other factors. This is justified by the capacity to attract potentials clients in biometrics and healthcare sector. The company's competitiveness gets the highest score among the factors, followed by the rest of factors.

Two outputs were obtained using standard scoring and the weighted scoring. Below are the presentation of DPMs according to individual Customer Types.

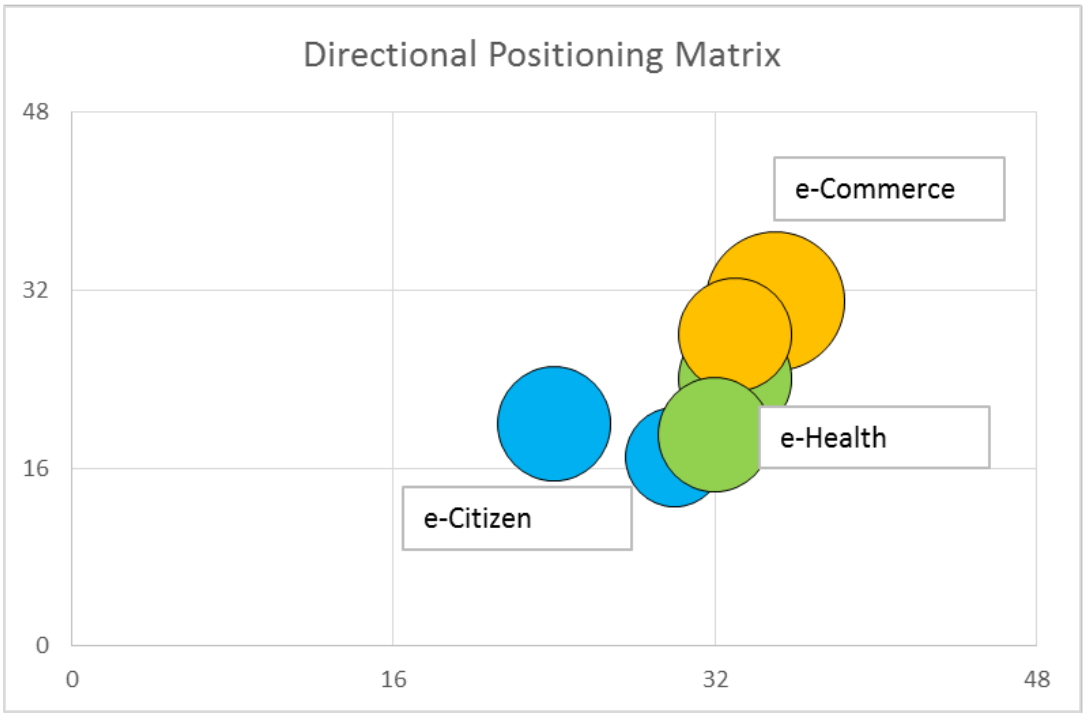

Figure 2: DPM for all five Customer Types colored according to segments (no weights applied)

Figure 2 shows that companies operating in the e-Commerce segment are in the strategically more advantageous position comparing to the companies or institutions involved in the e-Health and e-Citizen segments.

This suggests two things: first, the customers in the e-Commerce might not be willing to spend an extra cost on purchasing additional functionality unless this could help them to cut costs on

other components; second, on the contrary, the customers in the strategically less advantageous sectors (such as e-Health) might be willing increase their spending in the effort to improve their position both within a market and in terms of the company capabilities.

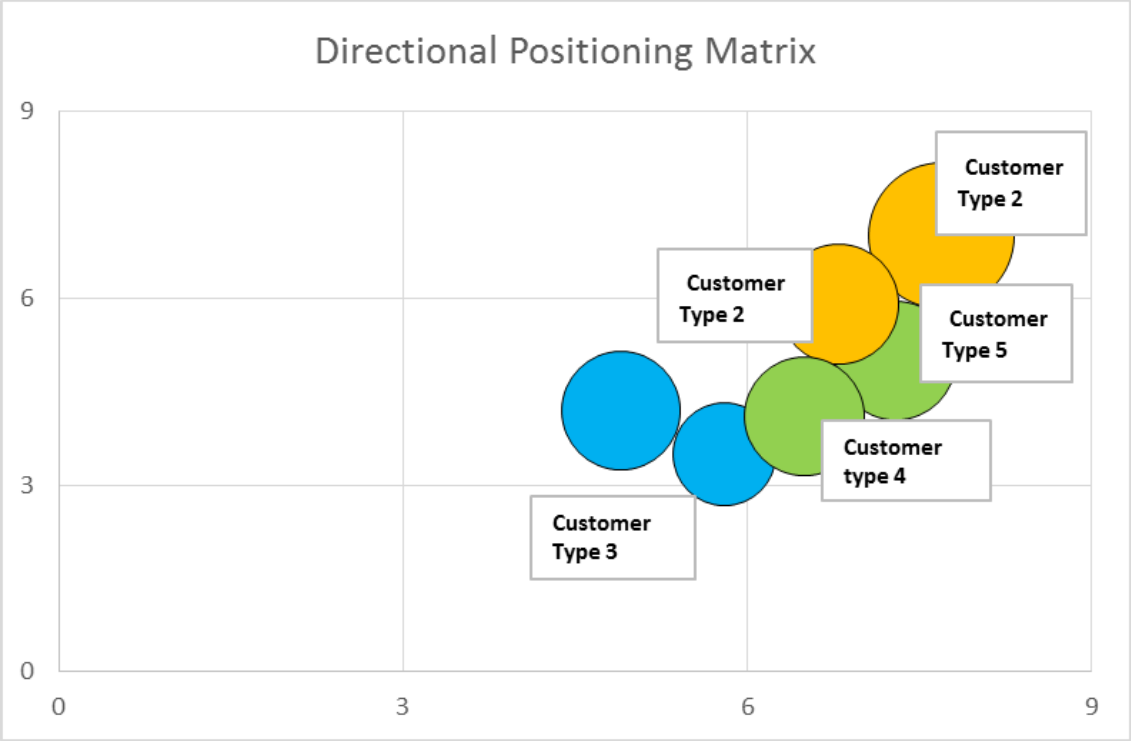

Figure 3: DPM for all five identified Customer Types (with weights applied): yellow bubbles indicate e-Commerce segment, green – e-Health, blue – e-Citizen

Figure 3 shows that Customer Type 2 (SDK buyers for mobile front-end applications for e-Commerce) occupies the most strategically advantageous position being followed up by Customer Type 3 (SDK buyers for existing systems for e-Commerce) and Customer Type 5 (Complex authentication system developers for e-Health).

Only Customer Type 2 is in a position which might require a sustainable effort in innovation, hence the need for novel authentication solutions. Customer Type 3 and Customer Type 5 are in a position where decisions need to be taken whether to continue chasing for leadership or phasing withdrawal. In both cases the offer from PIDaaS could be considered only if the proposed system could be a low-cost substitution for existing SDKs.

As concerning the rest of the identified Customer Types (Customer Types 3 and 4 – i.e., SDK buyers for existing systems for e-Health and e-Citizen segments respectively) these are in a position where additional investments in development are unlikely, yet there are needs for partnership with technology ventures such as start-ups in medical mobile applications which have not been yet identified as potential customers due to their low purchasing power, yet they could act as multipliers creating new channels for accessing those customers.

According to the DPMs, the recommendations have been defined according to the following grid (**Figure 4**):

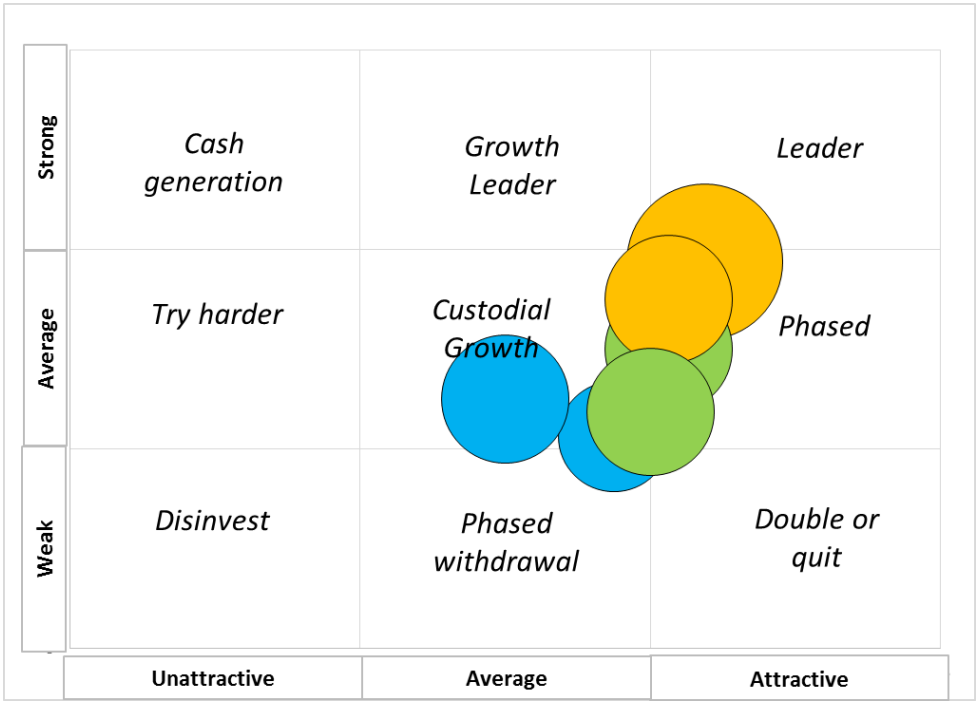

Figure 4: Strategic positioning of customer profiles according DPM

The tactics for each position are:

- Leader – Focus your resources on segments in this sector.
- Growth leader – Grow by focusing just enough resources here.
- Cash Generator – Milk segments in this sector for expansion elsewhere.
- Phased withdrawal – Move cash to segments with greater potential.
- Custodial – Do not commit any more resources to segments in this sector.
- Try harder –Determine if there are ways in which you can build your capability for segments in this sector for low levels of cash.
- Double or quit – Invest in your capability or get out of segments in this sector.
- Divest – Liquidate or move assets used in segments in this sector as fast as you can.

Hence, the recommendations are:

- Strategic position of PIDaaS applications for e-commerce: a mixed position between Leader and Phased Withdrawal.
- Strategic position of PIDaaS applications for e-citizen: a Custodial growth position.
- Strategic position of PIDaaS applications for e-health: a mixed position between Custodial growth, Growth leader and Phased withdrawal.

5 CONCLUSIONS

This section summarizes the conclusions and final remarks of the analysis & the strategic positioning of the PIDaaS platform.

5.1 PIDaaS Platform Analysis remarks

The integration of three technologies that are part of the PIDaaS platform presents itself as the biggest challenge of the project. A successful integration of these will allow obtaining a product at a big level of security, which will have to be complemented by a user's interface with big usability.

The time also is an important factor to keep in mind. It will be necessary that the development of the platform and the obtaining of a final product are realized in a few period that allow to be present on the market before other possible competitors are already implanted and there is gained the confidence of the providers of service and the final users.

5.2 SWOT Analysis remarks from the market perspective

PIDaaS provides an innovative approach to e-Services (e-Commerce, e-Citizen, and e-Health) in a way giving users strong advantages and market competitiveness in the following aspects (1) Convenience: PIN or password is omitted or expressed by voice; (2) Security: users are verified by their biometrics; and (3) Privacy protection: biometric information used for verification is protected by BTPS. These merits makes PIDaaS solution promising in the current and future markets because none of existing identity authentication solutions including those biometrics-enabled identity authentication solutions can perform well in all the three above aspects in the same time, which makes a good market perspective for the PIDaaS solution.

While the PIDaaS solution has the above mentioned strength and chances, we realize the following challenges facing an ever-changing market trend for digital identity management mechanism: (1) the platform's interoperability with various applications, mobile terminals, and computing environments, and to integrate different services; (2) cross-state market recognition; and (3) compliance to legislation and regulation requirements in different application fields. While these challenges act as market inhibitors to the PIDaaS solution, they are also market inhibitors to other competitive solutions in the current market. In this sense, we are optimistic about PIDaaS solutions market potential.

5.3 DPM Analysis remarks

The following conclusions could be reached from the DPM analysis:

- *Strategic position of PIDaaS applications for e-Commerce* is a mixed position between Leader and Phased Withdrawal depending on a customer type: Customer Type 1 is clearly in the Leader position, while Customer Type 2 is closer to Phased Withdrawal positions. In the first case more focus is needed on resources, hence PIDaaS exploitation strategy could address that; for Customer Type 2 companies are looking for alternative avenues for investing into new segments with greater potential; hence PIDaaS could be positioned as a solution to economize on resources internally and externally but also as opening entry into new application markets outside of e-Commerce (e.g. e-service retail such as e-Insurance);

- *Strategic position of potential customers of PIDaaS applications for e-citizen* segment is similar to the position of companies which we defined as belonging to Customer 2 – they are too looking for strategic openings in new segments outside of e-citizen, e.g. extending applications into e-health segment.
- *Strategic position of potential customers of PIDaaS applications for e-health* is identified as a mixed position between Growth leader and Phased withdrawal. On the one hand, given the current perspectives in healthcare market of biometric technology, security systems for health-related information access is becoming a worth investing segment with great potential. On the other hand, focusing enough resources in the segment of healthcare security systems may lead to a significant growth from a company's perspective.
  However, in some limited cases (where e-Health development is given a regional priority and is being supported with public investments opening market opportunities for e-Health IT solutions) a strategic position of potential customers of PIDaaS applications for e-Health sector could be defined as being in the position between a Custodial growth and Growth Leader. In this case the PIDaaS solution could help such companies to sustain their growth and value creation by contributing to the provision of personalized medicine.

5.4 Recommendations for Exploitation remarks

When considering a sales strategy, one needs to identify both a potential customer and a purchasing decision maker.

In many cases (especially as concerning the governmental sector or large corporations) a purchasing decision maker is Head of IT department inside the organisation and his interest is to preserve the existence of his IT unit intact while unloading most of the work through subcontracting.

Thus, when offering PIDaaS for sale, two sales strategies could be employed:

- First, a strategy to create a value proposition that could help heads of IT units inside of end-user organisations to be ahead of others by being able to directly implement PIDaaS SDKs, bringing additional conveniences and security to premium customers, without little need for external subcontracting for implementation of PIDaaS (to that end an easy installation procedures are needed).
- Second, a strategy of targeting companies which are offering complete multi-factor authentication solutions - to them we will need to highlight the advantages of PIDaaS that put them ahead of competition and create the possibility to earn extra money through repeated sales by offering system upgrades and maintenance -.

6 REFERENCES

[1] Research and Markets, Global Biometrics Market in the HealthCare Industry 2014-2018. *http://www.researchandmarkets.com/research/s59dzx/global_biometrics*, 2013.

[2] K. J. Annulis J, «Biometrics revolution in healthcare: where access and control of medical history shifts from provider to patient». *http://www.sciencedirect.com/science/article/pii/S0969476514701250*

[3] G. S, «Healthcare biometrics: solving the staff and patient security governance challenge». *http://www.sciencedirect.com/science/article/pii/S0969476513701437*

[4] The Chartered Institute of Marketing, «How to grow through new and existing customers», CIM 14280 (May 2009) *http://www.cim.co.uk/files/targetingcustomers.pdf*

7 ANNEX: DPM TABLES FOR EACH OF THE ANALYSED COMPANY

7.1 Strategic positioning assessment of pigu.lt

Factor	Weight	Max. Score	Your SCORE	Weighted
Size of the segment	0.2	10	**6**	1.2
Growth rate of the segment	0.3	18	**15**	4.5
Profit margins of the segment	0.1	5	**2**	0.2
Ongoing purchasing power of the segment	0.1	5	**3**	0.3
Attainable market share	0.2	5	**3**	0.6
Required market share to break even	0.1	5	**2**	0.2
Total	1	48	**31**	7

Table 4: Attractiveness Factors of pigu.lt

Factor	Weight	Max. Score	Your Score	Weighted
Competitive capability of the organization	0.2	14	**12**	2.4
Access to distribution channels	0.3	14	**10**	3
Capital and human resource investment required to serve the segment	0.1	10	**5**	0.5
Brand association of the organization in the eyes of the segment	0.3	5	**5**	1.5
Current market share/likely future market share	0.1	5	**3**	0.3
Total	1	48	**35**	7.7

Table 5: Capability Factors of pigu.lt

7.2 Strategic positioning assessment of Privalia

Factor	Weight	Max. Score	Your SCORE	Weighted
Size of the segment	0.2	10	**4**	0.8
Growth rate of the segment	0.3	18	**12**	3.6
Profit margins of the segment	0.1	5	**4**	0.4
Ongoing purchasing power of the segment	0.1	5	**3**	0.3
Attainable market share	0.2	5	**3**	0.6
Required market share to break even	0.1	5	**2**	0.2
Total	1	48	**28**	5.9

Table 6: Attractiveness Factors of Privalia

Factor	Weight	Max. Score	Your Score	Weighted
Competitive capability of the organization	0.2	14	**9**	1.8
Access to distribution channels	0.3	14	**9**	2.7
Capital and human resource investment required to serve the segment	0.1	10	**7**	0.7
Brand association of the organization in the eyes of the segment	0.3	5	**4**	1.2
Current market share/likely future market share	0.1	5	**4**	0.4
Total	1	48	**33**	6.8

Table 7: Capability Factors of Privalia

7.3 **Strategic positioning assessment of** BAIP

Factor	Weight	Max. Score	Your SCORE	Weighted
Size of the segment	0.2	10	**4**	0.8
Growth rate of the segment	0.3	18	**10**	3
Profit margins of the segment	0.1	5	**4**	0.4
Ongoing purchasing power of the segment	0.1	5	**3**	0.3
Attainable market share	0.2	5	**2**	0.4
Required market share to break even	0.1	5	**1**	0.1
Total	1	48	**24**	5

Table 8: Attractiveness Factors of BAIP

Factor	Weight	Max. Score	Your Score	Weighted
Competitive capability of the organization	0.2	14	**10**	2
Access to distribution channels	0.3	14	**12**	3.6
Capital and human resource investment required to serve the segment	0.1	10	**6**	0.6
Brand association of the organization in the eyes of the segment	0.3	5	**3**	0.9
Current market share/likely future market share	0.1	5	**2**	0.2
Total	1	48	**33**	7.3

Table 9: Capability Factors of BAIP

7.4 Strategic positioning assessment of Adeslas

Factor	Weight	Max. Score	Your SCORE	Weighted
Size of the segment	0.2	10	**4**	0.8
Growth rate of the segment	0.4	18	**6**	2.4
Profit margins of the segment	0.1	5	**3**	0.3
Ongoing purchasing power of the segment	0.1	5	**2**	0.2
Attainable market share	0.1	5	**2**	0.2
Required market share to break even	0.1	5	**2**	0.2
Total	1	48	**19**	4.1

Table 10: Attractiveness Factors of Adeslas

Factor	Weight	Max. Score	Your Score	Weighted
Competitive capability of the organization	0.2	14	**9**	1.8
Access to distribution channels	0.3	14	**8**	2.4
Capital and human resource investment required to serve the segment	0.1	10	**8**	0.8
Brand association of the organization in the eyes of the segment	0.3	5	**4**	1.2
Current market share/likely future market share	0.1	5	**3**	0.3
Total	1	48	**32**	6.5

Table 11: Capability Factors of Adeslas

7.5 Strategic Positioning Assessment of Government of Catalonia e-Citizen developments

Factor	Weight	Max. Score	Your SCORE	Weighted
Size of the segment	0.2	10	**4**	0.8
Growth rate of the segment	0.3	18	**8**	2.4
Profit margins of the segment	0.1	5	**2**	0.2
Ongoing purchasing power of the segment	0.1	5	**2**	0.2
Attainable market share	0.2	5	**2**	0.4
Required market share to break even	0.1	5	**2**	0.2
Total	1	48	**20**	4.2

Table 12: Attractiveness Factors of the Government of Catalonia e-Citizen developments

Factor	Weight	Max. Score	Your Score	Weighted
Competitive capability of the organization	0.2	14	**9**	1.8
Access to distribution channels	0.3	14	**5**	1.5
Capital and human resource investment required to serve the segment	0.1	10	**5**	0.5
Brand association of the organization in the eyes of the segment	0.3	5	**3**	0.9
Current market share/likely future market share	0.1	5	**2**	0.2
Total	1	48	24	4.9

Table 13: Capability Factors of the Government of Catalonia e-Citizen developments

7.6 Strategic positioning assessment of Registru centras

Factor	Weight	Max. Score	Your SCORE	Weighted
Size of the segment	0.2	10	**3**	0.6
Growth rate of the segment	0.3	18	**5**	1.5
Profit margins of the segment	0.1	5	**1**	0.1
Ongoing purchasing power of the segment	0.1	5	**1**	0.1
Attainable market share	0.2	5	**5**	1
Required market share to break even	0.1	5	**2**	0.2
Total	1	48	17	3.5

Table 24: Attractiveness Factors of Registru centras

Factor	Weight	Max. Score	Your Score	Weighted
Competitive capability of the organization	0.2	14	**10**	2
Access to distribution channels	0.3	14	**5**	1.5
Capital and human resource investment required to serve the segment	0.1	10	**7**	0.7
Brand association of the organization in the eyes of the segment	0.3	5	**4**	1.2
Current market share/likely future market share	0.1	5	**4**	0.4
Total	1	48	30	5.8

Table 15: Capability Factors of Registru centras