Impulse

Identity Management in PUbLic SErvices

# D4.6 Case study-based SWOT analysis of business models options


**Lead Author: Yan Xin**

**With contributions from: Antero Kutvonen**

**Reviewer: Nicholas Martin, Alicia Jiménez González, Mayra Ovando, Jaime Loureiro Acuña, and EAB experts Cristina Viano, Federica Russo, Laura Kask and Henk Marsman**


| | |
|---|---|
| **Deliverable nature:** | R |
| **Dissemination level: (Confidentiality)** | PU |
| **Delivery date:** | 21/12/2023 |
| **Version:** | 3.0 |
| **Total number of pages:** | 45 |
| **Keywords:** | Digital identity, facial recognition, SWOT analysis, business model |


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

# Executive summary

This deliverable conducts a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis of the IMPULSE eID solution and based on that, presents future business model alternatives for IMPULSE eID solution, as well as suggested actions under various models. As such, it is a combined report on the results of activities of both tasks *4.3. Case study-based SWOT analysis of business model options* and *4.4. Business model development and assessment*.

The research addresses the value creation and capture activities in complex networks of divergent actors (both public and private). In multi-stakeholder situations, such as in IMPULSE, defining the best possible business model(s) is not easy and requires simultaneously accounting for the context of the model as well as the divergent motivations and value perspectives of each of the involved stakeholders. Thus, the approach taken is to focus on the creation of archetypal business model(s) and estimating their sustainability in the short- and long-term.

The Deliverable first reviews the relevant literature on the adoption of eID solutions in general, with a focus on facial recognition technology. Based on that, it analyses the Strengths, Weaknesses, Opportunities and Threats of IMPULSE eID solution. Possible business model options in various scenarios are provided in the end to promote the adoption of IMPULSE eID solution, as well as to enhance/suggest its future development.

IMPULSE eID solution has the potential to be used in both the public and private sectors with a variety of business model options, provided that its strengths are taken into consideration, its opportunities are maximized, and the threats are minimized. The unique features of IMPULSE and the partners behind its creation enable the pursuit of short-term exploitation of project results through licensing and service business models that maximize learning opportunities and resource availability for the IMPULSE development while providing easy implementation to customers. Given sufficient development and favourable market conditions the long-term business models of IMPULSE could scale the business both for deeper and broader customer engagement over consulting and platform models.

# Document information

| | | | |
|---|---|---|---|
| **Grant agreement No.** | **101004459** | **Acronym** | **IMPULSE** |
| **Full title** | **Identity Management in PUbLic SErvices** | | |
| **Call** | DT-TRANSFORMATIONS-02-2020 | | |
| **Project URL** | https://www.impulse-h2020.eu/ | | |
| **EU project officer** | Jens HEMMELSKAMP | | |

| | | | | |
|---|---|---|---|---|
| **Deliverable** | **Number** | D4.6 | **Title** | Business model development and assessment |
| **Work package** | **Number** | WP4 | **Title** | Social and Economic Impact Assessment |
| **Task** | **Number** | T4.3/ T4.4 | **Title** | Case study-based SWOT analysis of business model options / Business model development and assessment |

| | | | | |
|---|---|---|---|---|
| **Date of delivery** | **Contractual** | M34 | **Actual** | M35 |
| **Status** | version 3.0 | | ☒Final version | |
| **Nature** | ☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot) | | | |
| **Dissemination level** | ☒Public ☐Confidential | | | |

| | | | | |
|---|---|---|---|---|
| **Authors (partners)** | Yan Xin and Antero Kutvonen (LUT) | | | |
| **Responsible author** | **Name** | Yan Xin | | |
| | **Partner** | LUT | **E-mail** | yan.xin@lut.fi |

| | |
|---|---|
| **Summary (for dissemination)** | SWOT analysis of IMPULSE eID solution and suitable case studies of business models and strategic guidelines for further use of the technologies in the socio-economic context |
| **Keywords** | Digital identity, facial recognition, SWOT analysis, business model |

**Version Log**

| Issue Date | Rev. No. | Author | Change |
|---|---|---|---|
| 13.11.2023 | 1.0 | Yan Xin & Antero Kutvonen | Full draft of deliverable for consortium internal peer review |
| 24.11.2023 | 1.1 | Nicholas Martin | Review; various minor language corrections, some suggestions for smaller changes to the text at various points to better specify certain arguments, direct implementation of some of these suggestions |
| 29.11.2023 | 1.2 | Alicia Jiménez Gonzáles | Review comments, some directly implemented |
| 1.12.2023 | 1.3 | Mayra Ovando | Review comments |
| 5.12.2023 | 1.31 | Jaime Loureiro Acuña | Minor review comments |
| 8.12.2023 | 2.0 | Yan Xin & Antero Kutvonen | Implementing peer review comments and finalizing deliverable for submission |
| 18.12.2023 | 2.1 | EAB experts Cristina Viano, Federica Russo, Laura Kask and Henk Marsman | Review comments |
| 21.12.2023 | 3.0 | Yan Xin & Antero Kutvonen | Implementing EAB comments and finalizing deliverable for submission |

# Table of contents

# List of figures

# List of tables

# Abbreviations and acronyms

| | |
|---|---|
| **DLT** | Distributed Ledger Technologies |
| **EBSI** | European Blockchain Services Infrastructure |
| **EC** | European Commission |
| **EU** | European Union |
| **eID** | electronic identity |
| **ETSI** | European Telecommunications Standards Institute |
| **GDPR** | General Data Protection Regulation |
| **ICT** | Information and Communication Technologies |
| **QES** | Qualified Electronic Signature |
| **QSCD** | Qualified Signature Creation Device |
| **SSI** | Self-Sovereign Identity |
| **SWOT** | Strengths, Weaknesses, Opportunities and Threats analysis |
| **FRT** | Facial Recognition Technology |

# 1 Introduction

This report is the final version of the Deliverable on SWOT analysis and business model options of the IMPULSE electronic identity (eID) solution (Deliverable 4.6). The main question intends to answer is, what archetypical business model options can be proposed to promote the adoption of the IMPULSE eID solution. To answer this question, the Deliverable conducted a systematic literature review on the adoption of eID solutions in general, with a focus on facial recognition technology. The benchmarking adoption scenarios were used to assess the Strengths, Weaknesses, Opportunities, and Threats (SWOT) of the IMPULSE eID solutions. Potential business model options in various scenarios are proposed to match IMPULSE's strengths with opportunities and to ward off threats, with the goal of promoting the adoption of IMPULSE eID solutions and enhancing/suggesting its future development.

The text is organised as follows. Chapter 2 presents the comprehensive literature review on the adoption of eID solutions and formulate the research questions. Following that, SWOT analysis of the IMPULSE eID solution is conducted in Chapter 3. Chapter 4 proposes the potential business model options for the IMPULSE eID solution in various scenarios. Finally, the Deliverable is concluded in Chapter 5.

# 2 Current status of eID adoption and research questions

IMPULSE, an eID solution with the function of biometric authentication/log-in (facial recognition), is undergoing pilot testing in six digital government cases. IMPULSE is currently a basic digital identity solution, but future development to qualify as an advanced digital identity is planned. As a result, this chapter will review literature on the adoption of both basic and advanced digital identity solutions.

## 2.1 Concepts of different eID solutions

Definitions/concepts of various eID solutions have been provided in D4.3. To make it easier to follow, relevant definitions/concepts are summarized in the current deliverable, as shown in Table 1.

**Table 1 List of concepts**

| Term | Definition/concepts | References |
|---|---|---|
| electronic identity, eID, digital identity<br>(The three terms are used interchangeably in this work) | An electronic/digital means that allows entities (citizens, businesses, machines, etc.) to prove who they say they are, via a digital channel. It is an identification representing unique attributes used for authentication and authorization in an electronic public or private service context. | European Commission n.d.[1]; White et al., 2019 |
| basic digital identity | An eID that enables only authentication. | Echikson, 2020; White et al., 2019 |
| advanced digital identity | An eID that allows additional information about the individual to be electronically stored in it or automatically linked to it (for example, via digital wallets). | Echikson, 2020; White et al., 2019 |

[1] https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf, Electronic Identities - a brief introduction

| | | |
|---|---|---|
| biometric identification | It is a method of identifying or confirming a person's identity based on the individual's unique physical, physiological or behavioural characteristics. | European Parliament[2], |
| facial recognition technology (FRT) | It is a technology that may be used to automatically recognize individuals based on his/her face, and it is often based on artificial intelligence such as machine learning technologies. Applications of FRT are increasingly tested and used in a variety of areas, ranging from individuals to business enterprises and public administration. | European Data Protection Board[3] |
| electronic signature | It is data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign, where the signatory is a natural person. | European Commission[4] |
| Qualified electronic signatures (QES) | A qualified electronic signature is an advanced electronic signature which is additionally:<br>▪ created by a qualified signature creation device (QSCD);<br>▪ and is based on a qualified certificate for electronic signatures. | European Commission[4] |
| digital signature | It refers to a mathematical and cryptographic concept that is widely used to provide concrete and practical instances of electronic signatures.<br>The definition given by ETSI TR 119 100 is that of '*data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient*.'<br>All electronic signatures are not necessarily digital signatures. | European Commission[5] |
| self-sovereign identity (SSI) | SSI is a concept associated with the way identity is managed in the digital world. According to the SSI approach, users should be able to create and control their own identity, without relying on any centralised authority. SSI is based on the use of Decentralised Identifiers. | European Commission[6] |

[2] https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces

[3] https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

[4] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+FAQ#eSignatureFAQ-Generalquestions

[5] https://ec.europa.eu/digital-building-blocks/wikis/display/ESIGKB/What+is+the+difference+between+an+electronic+signature+and+a+digital+signature, What is the difference between an electronic signature and a digital signature

[6] https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf, EIDAS SUPPORTED SELF-SOVEREIGN IDENTITY

## 2.2 Review strategy

To establish a comprehensive state-of-the-art understanding on the adoption of eID technologies, we employed a systematic literature review methodology. We conducted our literature search using the SCOPUS database, focusing on articles and conference proceedings. In our pursuit of pertinent literature regarding eID adoption across various domains, we refined our search within specific sections of the database, namely 'Social Sciences', 'Business, Management and Accounting', 'Economic, Econometrics and Finance', and 'Health Professions'. To maintain consistency with the search strings employed in D4.3, as well as to encompass the breadth of eID adoption areas, especially focusing on facial recognition technology, we executed two separate searches. These searches targeted articles with any of the following keywords in their titles or abstracts:

*1st set of search*

*Adoption AND (Digital identity OR electronic identity OR eID OR digital personal identity OR self sovereign OR sovereign identity OR SSI OR facial recognition OR biometric identification OR biometric identity)*

*2nd set of search*

*Application AND (Digital identity OR electronic identity OR eID OR digital personal identity OR self sovereign OR sovereign identity OR SSI OR facial recognition OR biometric identification OR biometric identity)*

In the 1st set of searches, we retrieved a total of 277 articles. Among these, 171 articles were sourced from the 'Social Sciences' section, 123 from 'Business, Management and Accounting', 36 from 'Economic, Econometrics and Finance', with no articles found in the 'Health Professions' category. In the 2nd set of searches, a more extensive selection of 1401 articles was obtained, comprising 960 articles from 'Social Sciences', 370 from 'Business, Management and Accounting', 148 from 'Health Professions', with no articles found in the 'Economic, Econometrics and Finance' section. After eliminating duplicate entries between the two searches, we meticulously reviewed the abstracts of the remaining articles to identify those aligning with the objectives of this deliverable. Finally, approximately 80 papers were included in our comprehensive study. While the number of available literature on the adoption of eID may initially appear substantial, a closer examination reveals a different reality. Many papers possessed only tangential relevance, such as technical papers proposing innovative eID solutions or largely conceptual papers lacking empirical data on the questions of primary interest. In response to this, our review incorporated an analysis of the references and footnotes within these papers, allowing us to identify additional sources, including pertinent 'grey literature'. In this review, we present a synthesis of the key findings and insights drawn from our analysis.

## 2.3 Adoption of eID solutions in public sector

A unique electronic identification (eID) enables citizens to perform various activities after authentication, achieved through a combination of attributes such as passwords, PINs, smartcards, tokens, biometrics, and more (Sule et al., 2021). In response to the imperative to dematerialize procedures and documents while ensuring access to e-Government services, e-Health services, and a spectrum of digital services proffered by both public and accredited private entities (Casalino et al., 2017), governments globally are progressively embracing eID systems.

On September 17, 2014, the regulation concerning the establishment of identification and trust services for electronic transactions within the internal market, known as eIDAS, came into effect and the plans for a

European digital identity was initially unveiled in 2019[7]. The European Union adopted eIDAS to create a structured framework for secure and reliable electronic identification and trust services. This framework ensures cross-border interoperability and facilitates secure and easy-to-use online interactions for both citizens and businesses when engaging with public and private services (European Commission, 2021). In 2021, an updated version, known as eIDAS 2, was introduced, enlarging its scope from relying on national digital identity schemes to encompass electronic attestations of attributes that hold validity at the European level. It further specifies that Member States would provide citizens and businesses with digital wallets capable of linking their national digital identities with proof of other personal attributes[8] [9]. The most recent provisional agreement reached by the Trologies (Commission, Council, and European Parliament) on the new framework for European digital identification (eIDAS 2.0) on November 8th, 2023[10], acknowledged electronic ledgers as trusted services. Furthermore, as part of the Digital Compass plan introduced in 2021, EU member states have been tasked with the objective of ensuring that 80% of their citizens will be utilizing digital identities by the year 2030[11].

In all European countries, eID systems are supported by local governments (Casalino et al., 2017). While these systems hold the promise of providing secure and supposedly easy-to-use ways for electronic identification, it is noteworthy that, despite the recognition of the necessity for digital identities in most member states, only 14 out of the 28 European Union member states have adopted eID systems in alignment with the established regulations (Guggenberger et al., 2023). It should be highlighted, however, that eID solutions are highly contextual and operated in a socio-economic environment. A detailed analysis of the social and economic impact of eID solutions can be found in D4.4 Economic Benefits of the IMPULSE Approach - V2.

Upon closer examination at the national level, the adoption of government-provided eID services remains notably low. As an illustrative case, merely 7% of German citizens have engaged with the German eID system to date (European Commission, 2021). However, it is imperative to acknowledge the pioneering efforts in eID adoption by countries such as Estonia, Finland, and Belgium. A comprehensive survey of digital identity initiatives across Europe would be remiss without highlighting Estonia's exceptional achievements in this domain. Estonia embarked on its eID journey nearly two decades ago. According to official reports from the Estonian government, 99% of its services are accessible online, and compelling evidence supports the actual utilization of these online services[12].

Considering the digital identification methods used in public sector, various approaches have been adopted. For instance, the e-residency program[13] in Estonia provides digital identity cards (smartcards) to non-residents to enable secure access to government services and e-commerce, using PIN codes and fingerprints for authentication. The eID system in Dutch government, DigiD[14], is primarily based on a username and a password to access a range of public services, including healthcare and tax-related services. Beyond Europe, India has one of the largest biometric eID systems in the world, Aadhaar program[15]. It collects biometric data

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=ES, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

[9] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf, Revision of the eIDAS Regulation Findings on its implementation and application

[10] https://www.consilium.europa.eu/en/press/press-releases/2023/11/08/european-digital-identity-council-and-parliament-reach-a-provisional-agreement-on-eid/, European digital identity: Council and Parliament reach a provisional agreement on eID

[11] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en, Europe's Digital Decade: digital targets for 2030

[12] https://e-estonia.com/solutions/e-governance/government-cloud/, e-Governance

[13] https://www.e-resident.gov.ee/, Your digital ID, your company, your freedom

[14] https://www.government.nl/topics/online-access-to-public-services-european-economic-area-eidas/everything-you-need-to-know-about-eidas

[15] https://www.chandlerinstitute.org/governancematters/indias-aadhaar-system-bringing-e-government-to-life

(fingerprint and iris scans) and issues a 12-digit Aadhaar number to citizens. Users can use biometrics or receive a one-time password (OTP) on their registered mobile number to get authentication to a wide range of public services. In Singapore, although the eID system, SingPass[16], is primarily based on a username and password, a two-factor authentication (2FA) is required for accessing sensitive services.

When contemplating the adoption scenarios of eID in the public sector, its primary utilization is observed in e-government, e-health, law enforcement, and border control.

Regarding eID adoption in e-government, as previously discussed, e-government initiatives aim to provide citizens with online access to government services, eliminating the need for in-person visits and relying on the associated eID credentials. Estonia serves as a notable success story, having offered e-government services to its citizens for over a decade. In 2016, Italy introduced its Public Digital Identity System (SPID)[17] to facilitate rapid, secure access to digital services offered by both local and central administrations. However, in its early days, SPID has encountered challenges related to adoption progress (Casalino et al., 2017). In response to the main challenge in the eID card application process, namely, the long waiting times for registry appointments, an application was launched to mitigate waiting times. This app streamlines the preliminary stages of eID card requests via smartphones, ultimately reducing waiting times (Sule et al., 2021). As of late November 2022, about 63% of the Italian adult population had a SPID identity[18].

Beyond e-government, the implementation of e-health solutions offers governments the opportunity to exert greater control over local infrastructures, optimize resource allocation, and enhance the efficiency of public fund utilization(Casalino et al., 2017). Again, Estonia serves as a prominent exemplar in the e-health domain. All individuals entitled to the National Health Service in Estonia are equipped with a national health record, accessible through credentials linked to their eID. The utilization of the ePrescription platform ensures that all interactions, electronic prescriptions, and communications between healthcare providers and patients occur within a secure channel, accessible through appropriate credentials[19]. This approach has not only improved patient care but also alleviated administrative burdens while fortifying data security. In the Netherlands, the MyDignity platform (known as Mijn Dossier in Dutch) empowers patients to access their medical records and engage in direct communication with healthcare professionals[20]. This facilitates active patient involvement in their healthcare and bolsters communication between patients and healthcare providers. Finland has mandated the use of the ePrescription System since 2017, requiring all prescriptions to be processed through this electronic system[21]. This transition facilitates electronic prescribing and dispensing of medications, streamlining the healthcare process.

Electronic identification has found application within law enforcement authorities on a global scale (Eneman et al., 2022; Matulionyte, 2023). For instance, the United States features the National-level Automated Fingerprint Identification System (AFIS)[22], a critical component of the U.S. criminal justice system. AFIS plays a pivotal role by collecting and storing biometric data in the form of fingerprint images, greatly assisting law enforcement agencies in the identification and apprehension of individuals involved in criminal activities. It also provides valuable support in criminal investigations. Within the European Union, the European fingerprint database known as EURODAC serves as an essential tool for the identification and verification of individuals, ensuring that asylum applications are not submitted in multiple EU countries[23]. Introduced in 2003, EURODAC is employed by 32 countries, comprising the 28 EU Member States and four Associated Countries

[16] https://www.singpass.gov.sg/main/, Your improved digital ID to make life easy.
[17] https://www.spid.gov.it/en/, spid, Your digital identity
[18] https://www.namirial.com/en/news/digital-identity-state-of-play-italy-end-of-2022/#:~:text=Usage%20of%20Italian%20Public%20Digital%20Identity%20System&text=In%20late%20November%202022%20the,24%20activated%20their%20digital%20identity, Usage of Italian Public Digital Identity System
[19] https://e-estonia.com/solutions/healthcare/e-prescription/
[20] https://mijndossier.amsterdamumc.nl/MyChart-PRD/Authentication/Login?
[21] https://www.eu-healthcare.fi/medicines/finnish-prescriptions/
[22] https://www.ojp.gov/pdffiles1/nij/225326.pdf, Automated fingerprint identification system (AFIS)
[23] https://eur-lex.europa.eu/EN/legal-content/summary/eurodac-european-system-for-the-comparison-of-fingerprints-of-asylum-applicants.html, Eurodac: European system for the comparison of fingerprints of asylum applicants.

(Iceland, Norway, Switzerland, and Liechtenstein). EURODAC enables information sharing among EU Member States and fosters collaboration among EU law enforcement agencies and asylum authorities in the identification and tracking of individuals.

Facial recognition technology has witnessed significant advancements, leading to its related eID increased adopted for border control purposes. One notable initiative in this domain is iBorderCtrl, which is supported by funding from the European Commission under the H2020 framework. The primary objective of this initiative is to implement a system designed to expedite border crossing for pre-registered, legitimate travelers. This development aligns with the European Commission's broader initiative to establish a Schengen-wide frequent traveler program (Carlos-Roca et al., 2018).

In summary, the digital identity ecosystem holds the promise of enhancing efficiency, reducing fraud, lowering administrative and operational cost, and improving security and enhancing privacy (Sule et al., 2021). Nevertheless, its adoption remains somewhat limited within the European Union. In 2020, the European Commission initiated a study to investigate the factors contributing to the relatively low adoption of digital identities in European countries (European Commission, 2020). The study's findings highlighted the inadequacy of the existing European identity network in meeting the evolving requirements for digital identities. In response, eIDAS 2.0 is introduced, which leverages decentralized identifiers and modern cryptographic techniques to enhance privacy and security. Simultaneously, it strives to simplify access to a broad spectrum of digital services for both citizens and businesses (Guggenberger et al., 2023). This system is designed to augment the existing identity management infrastructure by facilitating the exchange of identity data between public institutions and private enterprises (European Commission, 2021).

## 2.4 Adoption of eID solutions in the private sector

While eID is is commonly associated with the public sector, it is also utilized in a variety of private sector applications, including financial services, healthcare, education, and tourism and hospitality. In line with IMPULSE's identification strategy, we will concentrate on eID adoption in private factors facilitated by face recognition technology (FRT).

Financial services

In recent years, biometric technologies have been widely embedded in mobile devices to enhance the security of mobile devices. With the rise of financial technology (FinTech), which uses mobile devices and applications as promotional platforms, biometrics has the important role of strengthening the security of the identification methods such applications employ. In particular, face recognition is the most preferred identification method in FinTech applications, compare to other biometric identifications including voice recognition, fingerprint recognition, and iris recognition, due to its ease of use and high security (Wang, 2021). Although fingerprint recognition presents relatively stable performance, thus explaining why it has a greater market share, most consumers consider that face recognition will have more merit in the future (Wang, 2021). With the popularity of smart phones, mobile payment is in some countries becoming the main payment method, gradually replacing cash payment and bank card payment (L. L. Zhang & Kim, 2021). Currently, many banks and financial institutions offer mobile banking apps with eID features (Baby Shamini et al., 2022). For instance, in HSBC UK, customer can use fingerprint or face recognition to log on faster to its Mobile Banking app or generate a security code on her/his Digital Secure Key[24]. In Bank South Australia, in addition to use 4-digit security number or password, users can use facial recognition or fingerprint to access the everyday banking needs quickly and securely[25].

[24] https://www.hsbc.co.uk/ways-to-bank/mobile/biometrics/#:~:text=Important%20security%20information,faces%20registered%20on%20your%20device , Use your biometrics to log on to the mobile banking app

[25] https://www.banksa.com.au/online-services/mobile-banking/quick-logon, Enable Quick logon in BankSA App – Fast and secure logon to BandSA App with FaceID, fingerprint, or a 4-digit security number.

Healthcare

In addition to the adoption of eID solutions in public healthcare, it is also adopted in private healthcare.

The importance of individual verification is advancing along with the advancement of mobile and health information systems (Abdul et al., 2017), and online healthcare applications have grown more popular over the years. Especially due to the Covid-19 pandemic, physical interactions are expected to be kept at a minimum, which boost the adoption of various online health applications. It was found that the demand for remote health care services increased by 50% in the first quarter of 2020 as compared to the same period in 2019 (Koonin et al., 2020). Those increase can be reflected from the adoption of Telehealth, an online healthcare application that allows patients and doctors to schedule consultations, prescribe medication, share medical documents, and monitor health conditions conveniently by using facial recognition authentication as it is convenient and accessible for people (Lin et al., 2022). Even without pandemic, eID solutions have been widely utilized in private heathcare. For instance, Swedish digital healthcare provider KRY offers remote medical consultations and prescriptions[26]. Patients can use the KRY app to access healthcare services by authenticating themselves using BankID in Sweden. However, it should be noted that, due to the vital patient information (i.e., the background of the patient, medical records, and medical images) stored and used, privacy and data protection are thought to present challenges for the use of FRT for health applications (Martinez-Martin, 2019).

Education

Digital identity related adoption in education is broad, but mainly focusing on attendance and participation tracking, online exam, and campus monitoring (Alzaabi et al., 2023; Crow et al., 2017; Da Costa Rocha et al., 2023; Jayakumar et al., 2022; Rachel et al., 2022; Sukmandhani & Sutedja, 2019). The proper adoption of such eID related applications can lead to beneficial effects for different stakeholders. From the students' perspective, it can enhance their academic experience by enabling more convenient routine interactions and motivating participation. However, the benefits are contingent on the thoughtful and context-sensitive implementation of the technology, without which it may instead lead to adverse behavioral adaptations such as 'chilling effects' or a focus on projecting participation instead of learning content. From the faculty viewpoint, the solution allows them to finish their tasks quicker and eliminate human error, but may also introduce novel ethical, educational and psychological questions. Therefore, initial implementation in education should be directed to the higher education level, where students have better capabilities to offer input and feedback to contextualize the implementation. In addition to these applications, various universities have invested in studying blockchain-based diploma systems to overcome the drawbacks of paper-based certificate, such as difficult to carry, easy to lose, and easy to forge. Therefore, in order to strengthen the connection between the diploma and the recipient, a blockchain deployment framework composed of educational authority and institutions is proposed to make the identity of the diploma issuer credible (Hsu et al., 2022). Although not fully employed, such system would have potential market even in the current time.

Tourism and hospitality

The application of the facial recognition systems by the tourism and hospitality industry has resulted in high expectations. For instance, in the case of the hospitality industry, facial recognition system (FRS) is a fast and effective system for authentication to improve conventional services and can also enhance hotel security. According to data from Marriott International, it takes an average of three minutes for each guest to check in using conventional methods. When there are many guests, however, they may need to spend considerable time waiting in line. Through the use of FRS, guests' check-in time can be reduced to 60 seconds, and waiting time for check-in can be greatly shortened (Wang, 2018). In addition, by providing automatic authentication, the adoption of FRS in hotel can improve security (NEC Corporation, 2020).

[26] https://www.kry.se/en/, Healthcare you can rely on.

## 2.5 Research questions

Based on the review of the current adoption status, three research questions are promote the adoption of IMPULSE:

1) What are the Strengths, Weaknesses, Opportunities and Threats for IMPULSE eID solutions?
2) What value can be created with the adoption of IMPULSE, and for whom?
3) What archetypical business model options can be proposed to promote the adoption of IMPULSE eID solutions?

# 3 SWOT analysis

To promote its adoption, SWOT analysis of IMPULSE is conducted in this chapter. The analysis will be based on the literature, as well as the output from D4.3. Before starting the analysis, the essential elements and objectives of SWOT analysis will be illustrated.

## 3.1 The definition and objective of SWOT analysis

Originated in the early 1950s at Harvard Business School, SWOT analysis was used by professors George Albert Smith Jr. and C Roland Christensen to examine organizational strategies in relation to their environment (Chermack & Kasshanna, 2007). Due to its effectiveness in analyzing the critical internal and external aspects that influence companies' strategic choice SWOT has remained a dominant analysis framework for decades (Hoskisson, 1999). The internal aspects are those that are within the control of the business, whereas the external aspects are those that the business cannot control (Bull et al., 2016; Hill & Westbrook, 1997). Based on a combination of Strengths, Weaknesses, Opportunities, and Threats, SWOT analysis can efficiently indicate alternative solutions for a company (Valentin, 2001; Weihrich, 1982).

## 3.2 Strengths of IMPULSE

Strengths are '*capabilities that enable your company or unit to perform well – capabilities that need to be leveraged*' (Harvard Business Review, 2005, p.25). The following questions serve as our guidelines for the analysis.

- What advantages does IMPULSE have?
- What distinguishes IMPULSE from other apps?
- What is IMPULSE's distinct selling point?

Considering the internal distinct advantage, Strengths of IMPULSE can be reflected from its unique qualities and the available resources, and most of them are easy to follow (as shown in Figure 1).


**Figure 1 Strengths of IMPULSE**

### 3.2.1 Unique qualities

IMPULSE's unique qualities include: security and convenience, cheap (for end users), interoperability with other systems in Europe (EBSI), contactless and hygienic, scalability, and potential to realize microcredentials (better privacy management). Although some contextual factors, such as internet access and the use of a smartphone with specific features, are prerequisites for experiencing the unique qualities identified, we can reasonably assume that the addressed market[27]has internet access and smartphones. According to Eurostat, the share of EU internet users in 2023 was 92%, and 85% of EU internet users connected to the internet by mobile phone or smarphone[28].

Security and convenience

As an SSI system, IMPULSE reduces complexity of integration with partners and provide a better customer experience (Richter & Anke, 2021). SSI systems also facilitate improved control of citizens over their identity by allowing them to define which property is shared with whom granularly thus preserving user privacy (Renduchintala et al., 2022; Sullivan & Burger, 2017).

IMPULSE is secure and convenient since it not only allows users to manage their own identities, but also makes it easier for them to access the important services without having to visit a dedicated office. Especially for handicapped citizens, IMPULSE can be more user-friendly than traditional identity (e.g., PIN) or other biometric identity (e.g., fingerprint authentication) (Otti, 2016). In addition, it eliminates the need to remember a password or carry an encrypted token (Sara Philomin et al., 2022).

Cheap (for end user)

[27] Addressed markets are typically less than 100% of the demographic due to a mix of contextual and human factors leading to the existence of a small non-adopting minority for most innovations, including eIDs
[28] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Use_of_e-government

The proliferation of different types of cameras makes capturing facial attribute straightforward and cheap (Beltrán & Calvo, 2023). Meanwhile, it makes facial image capture enrollment procedures easy and cheap to be implemented (Carlos-Roca et al., 2018). While it is possible to physically collect issued documents in an analog process, it is associated with high costs or even completely impracticable if the document can be copied at will (Guggenberger et al., 2023). For instance, IMPULSE does not require the use of a desktop computer, and also potentially eliminates some expenses such as postage and certain hardware.

Interoperability with other systems in Europe (EBSI)

As an SSI system, IMPULSE arguably puts users back in control of their own digital identity (for a dissenting view see Martin 2023). This will not only strengthen the position of the users but also provide benefits from an interoperability and process perspective (Richter & Anke, 2021; Toth & Anderson-Priddy, 2019). IMPULSE is built on a distributed electronic ledger (EBSI) that with the recent developments of eIDAS 2 are considered trusted services by the European Commission. This implies the potential for IMPULSE in terms of both competitiveness and compliance. In the long term, IMPULSE potentially will achieve better interoperability with other municipalities' digital public service provision systems.

Contactless and hygienic

In contrast to alternative identification methods like fingerprints and smart cards, the IMPULSE solution distinguishes itself by its contactless and hygienic attributes, primarily enabled through facial recognition technology. This feature holds particular advantages in specific scenarios and contexts, where health and safety concerns are paramount, as exemplified during the course of a pandemic or within healthcare settings.

Scalability

The extensive utilization of smartphones, coupled with their influence in familiarizing users with the acceptance of facial recognition technology, has the potential to significantly expedite the broader implementation of IMPULSE. This alignment with prevalent mobile device trends creates favorable conditions for IMPULSE to gain traction and acceptance among a wider audience.

Potential to realize microcredentials – better privacy management

One critical aspect to underline here is IMPULSE's potential to realize micro-credentials, which not only enables better privacy management but also aligns with the OECD strategy of promoting micro-credentials in education, training and labor markets (OECD, 2023), making IMPULSE more appealing.

### 3.2.2 Human resources

The human resources behind IMPULSE can be seen as a strength from both the personnel and the collaboration perspectives.

Skilled, knowledgeable experts

From a resource standpoint, IMPULSE benefits from a highly proficient and informed workforce that brings together multidisciplinary expertise, backgrounds, and diversity. The skilled experts play a pivotal role in driving the project's objectives forward and their achievement. Through the collaboration IMPULSE has created substantial new expertise that can be further recombined with other European excellence in digital identities to further develop projects and commercial solutions.

Smooth and efficient internal collaboration

The collaborative environment within the IMPULSE consortium deserves attention. The project's success is underpinned by the smooth interaction and coordination among consortium members, fostering the exchange

of ideas, resources, and insights. This collaborative synergy enhances project efficiency and promotes innovative solutions and knowledge sharing both in achieving the project's intended outcomes and supporting further exploitation.

## 3.3 Weaknesses of IMPULSE

Weaknesses are '*characteristics that prohibit your company or unit from performing well and need to be addressed*' (Harvard Business Review, 2005). The following questions serve as our guidelines for the analysis.

- What are the things where IMPULSE is weaker than competitors?
- What are the resource limitations of IMPULSE?

Weaknesses of IMPULSE can be classified to initially limited features, resource limitations, and the communicability of value created (as shown in Figure 2).

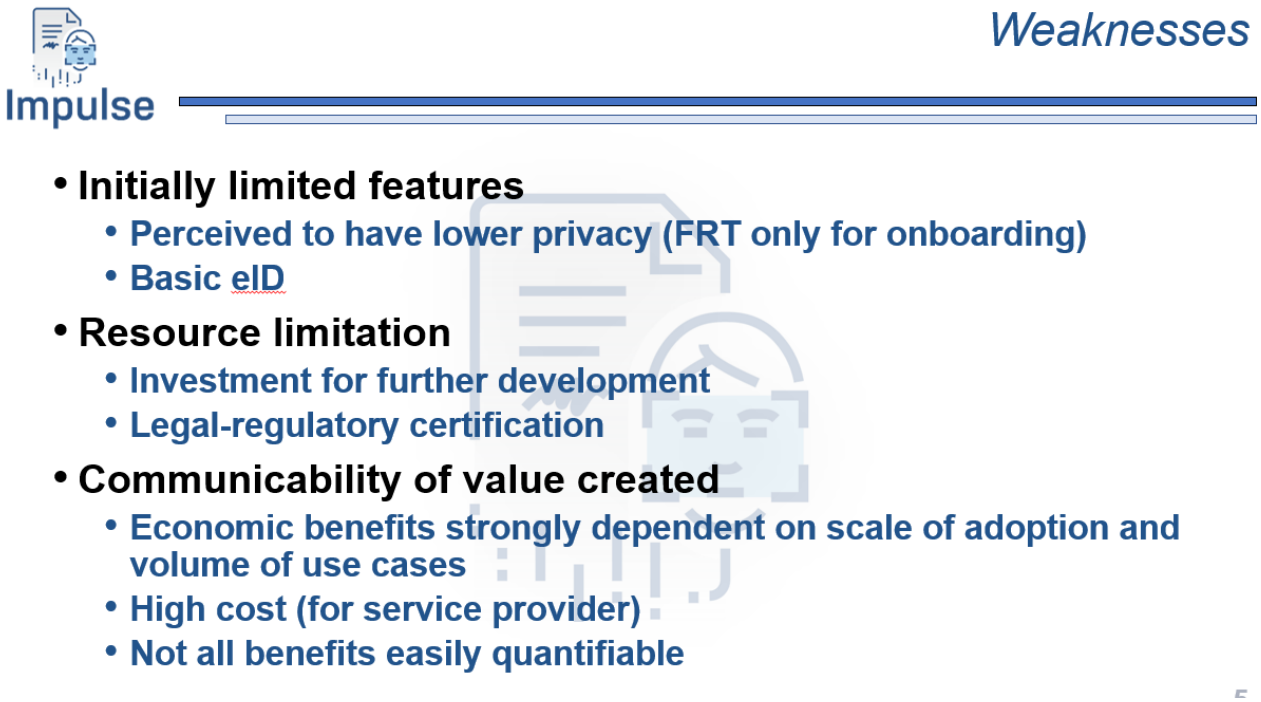


**Figure 2 Weaknesses of IMPULSE**

### 3.3.1 Initially limited features

When compared to features offered by competing solutions, IMPULSE's weaknesses include perceived lesser privacy and having only basic eID functionality initially.

Perceived to have lower privacy (FRT only for onboarding)

Privacy preservation is one of the significant challenges raised from the introduction of biometrics due to the highly sensitive nature of the data used (North-Samardzic, 2020; Sharma et al., 2023). As an eID solution using facial recognition on mobile phones, IMPULSE can be perceived by users to offer insufficient privacy compared to for example using token identification, which may complicate gaining trust of the users. However, facial recognition is only actually necessary when onboarding IMPULSE for the first time, and the files utilized in the process are immediately deleted. Therefore, the users keep control of their own data, implying a higher level of privacy when using IMPULSE (Chadwick et al., 2019; Richter & Anke, 2021). Communicating this successfully to new potential users will be important for counteracting the perceived weakness.

Basic eID

The IMPULSE solution at present is a tool to provide people only with a basic digital identity, meaning that the current version of IMPULSE enables only authentication and does not include a qualified electronic signature (QES) function, nor does it include a digital wallet to store certain types of user information, such as payment information, credentials or certificates, including electronic versions of physical documents like driver's licenses or university records. Both QES and digital wallet are important in relation to marketing IMPULSE. For instance, the ability to provide legally binding digital signatures is likely crucial to enable many higher-value use cases in both the public and private sector (e.g. taking on mortgages, applying for various permits). Meanwhile, with the development of modern digital identity systems, a digital wallet allowing users to digitally present and prove their possession of diverse certificates and credentials will be the trend.

### 3.3.2 Resource limitation

From resource limitation perspective, investment will be required for further development of IMPULSE. More legal-regulatory certification will be necessary as a result of the development.

Investment for further development

As previously discussed, the current instantiation of IMPULSE serves as a basic eID solution, lacking the functionalities of Qualified Electronic Signatures (QES) and digital wallet. To align with the evolving landscape of modern digital identity systems and extend its application range, plans are in place to upgrade IMPULSE, transforming it into an advanced eID solution. However, this prospective transition necessitates a substantial investment from both a human resource and financial perspective. The financial investment need is related largely to research and development and technology infrastructure costs. From a human resources perspective, developing, deploying, and maintaining advanced eID functionalities demands a highly skilled team of developers, cybersecurity experts, legal consultants, and customer support personnel.

Legal-regulatory certification

Even if it is to only serve as a basic eID solution, the deployment of IMPULSE necessitates compliance with a complex web of legal and regulatory frameworks, particularly concerning data protection and privacy, as IMPULSE is an FRT-based solution. In relation to the development of IMPULSE from basic eID to advanced eID will introduce an increased legal-regulatory certification requirement that is further amplified by the stringent regulations within the European Union (EU). Furthermore, the evolving nature of data protection and digital identity laws further compounds the complexity, requiring continuous adaptation and resource allocation to maintain compliance. Failure to meet these requirements could lead to legal complications and jeopardize the solution's validity and trustworthiness. Therefore, in the context of the EU, where digital identity and electronic signatures are heavily regulated, the legal-regulatory certification requirement poses a significant challenge for IMPULSE when transitioning from a basic eID to an advanced eID solution.

### 3.3.3 Communicability of value created

In terms of successful exploitation and commercialization, a key weakness of IMPULSE is the difficulty in effectively communicating the value created. This includes the inability of the solution to generate economic benefits in a short term or on a small scale, the potentially high cost (for service providers) to implement it, and the difficulty in quantifying the non-monetary benefits associated with its use.

Economic benefits strongly dependent on scale of adoption and volume of use cases

The economic impact analysis of IMPULSE (Deliverables 4.3 and 4.4) found that in the pilot cases, the economic benefits IMPULSE delivers per transaction (e.g. per document submitted to the municipal authorities

using IMPULSE rather than via existing channels) is small. This goes for both the benefit delivered to the citizen/consumer and to the enterprise/government agency. Economic benefits only become more substantial once IMPULSE is used for very many transactions. This in turn necessitates (i) high levels of adoption of IMPULSE by private citizens/users (>~75 percent), and (ii) ensuring that IMPULSE can be used for a very large number of different use cases. In other words, only with critical mass can the solution achieve substantial cost savings and an acceptable return on investment for the customer. Scale of adoption is thus important for evaluating possible business model options for IMPULSE. Furthermore, certain advantages of IMPULSE, particularly those associated with user experience enhancement, may not yield immediate economic benefits but rather contribute to long-term economic gains.

High cost (for service providers)

From the end-user's perspective, using IMPULSE means lower cost, as we discussed in section 3.2.1 Unique quality of this Deliverable. However, from a service provider's standpoint, the implementation and operation of SSI system like IMPULSE is high, which will be a challenge and hinders its adoption by both public and private sectors. The high cost may be due to a lack of reusable, production-ready components such as integration tools and software libraries (Richter & Anke, 2021), the cost of control, conversion and maintenance of the eID system as well as human effort (Casalino et al., 2017). For instance, the initial setup of a new SSI-based pan-European IdM alone is estimated to cost more than 600 million euros, plus the operating costs for public and private organizations during the period of use (European Commission, 2021). The high cost had been reflected from the pilot case, i.e. Aarhus Pilot.

Not all benefits easily quantifiable

IMPULSE offers a range of quantitative and qualitative benefits. Some of these are easier to obtain numerical estimates for than others. Arguably the most important directly quantifiable benefit are time and (labour) cost savings. These have been estimated for the pilot cases (cf. Deliverables 4.3 and 4.4), but as noted above, they start becoming substantial only when adoption levels are high and the volume of use cases large. Further benefits are quantifiable in theory, but in practice very hard to measure ex ante and, due to the problem of causal inference, even ex post. These include for example security benefits, enhanced transaction volumes and possible fraud reduction. Finally, there are a range of largely qualitative benefits that IMPULSE may have, which by nature resist numerical expression. These include improved user experiences, possible increases in trust and even greater quality of life if digital and bureaucratic processes become easier and more free of hassle.

## 3.4 Opportunities for IMPULSE

Opportunities are '*trends, forces, events, and ideas that your company or unit can capitalize on*' (Harvard Business Review, 2005, p.25) relating to the operating environment. The following questions serve as our guidelines for the analysis.

- What good opportunities can we spot for IMPULSE?
- What interesting trends are we aware of?

Opportunities of IMPULSE can be reflected from both the market's and the ecosystem's perspectives (as shown in Figure 3).


**Figure 3 Opportunities for IMPULSE**

### 3.4.1 Market

The market defines where IMPULSE will be supplied. Market opportunities for IMPULSE include growing demand for digital transformation, the requirement for high level security, the popularity of private FRT use, acceptance potential is higher in more sensitive/security-dependent contexts, and more trust on government and law enforcement agencies.

Growing demand for digital transformation

The rising demand for digital transformation underscores the rapid evolution of technology and a shifting landscape of consumer behaviours and expectations. This technological growth is important for any country and presents an opportunity for the widespread adoption of eID solutions (Casalino et al., 2017). From a market perspective, IMPULSE is well-positioned to leverage these opportunities. Organizations across both the public and private sectors now recognize the necessity of enhancing identity verification and access control processes. The increasing demand for remote and contactless services in today's digital environment positions FRT-based eID solutions, like IMPULSE, as crucial enablers that align with the contemporary market's emphasis on seamless and contactless interactions. With consumers embracing digital experiences, the demand for FRT-enabled eID solutions, such as IMPULSE, is growing, driven by the market's need for enhanced security, user convenience, and regulatory compliance. Consequently, businesses, particularly those in the private sector, are proactively integrating FRT-enabled eID solutions like IMPULSE into their digital strategies to remain competitive in a market where identity protection and privacy are paramount concerns.

Requirement for high levels of security

From a market perspective, the demand for FRT-enabled eID solutions like IMPULSE stems from the imperative need for enhanced security. Organizations spanning government, finance, and healthcare sectors have a shared recognition of the critical significance of fortifying the security of sensitive digital transactions and interactions. FRT offers robust identity verification capabilities that are inherently resistant to counterfeiting (Guggenberger et al., 2023). Consequently, FRT-enabled eID solutions like IMPULSE serve as a compelling means to elevate security in sectors like finance, government, and healthcare, where upholding rigorous security standards is of paramount importance. This creates market opportunities for IMPULSE to

address the escalating demand for secure, fraud-resistant identity verification across industries, while concurrently navigating the complex terrain of privacy and ethical considerations.

Private usage of FRT is popular

Facial recognition technology (FRT) has gained widespread acceptance and familiarity among the general population, primarily through its applications in consumer devices like smartphones. With the ubiquitous availability of mobile technology and the growing popularity of mobile apps for connectivity, these technologies have become integral to daily life (J. Zhang et al., 2018). Global mobile app downloads have shown a consistent upward trajectory since 2016, surpassing 255 billion in 2022 (Statista, 2023). Recent studies have highlighted that over 90% of young adults (aged 18 to 30) in Portugal use mobile apps daily (Simões et al., 2023), employing various authentication methods, including passwords, fingerprint recognition, facial recognition, and voice recognition. Moreover, as users become increasingly at ease with FRT, businesses can significantly enhance the customer experience by providing secure and convenient access to services. This trend opens doors for IMPULSE to leverage the existing affinity for FRT in the private sphere and drive its adoption in sectors that demand advanced security and user-friendly authentication methods. Research indicates that FRT acceptance is generally higher among younger, highly educated, and higher-income populations (Kostka et al., 2021), which might help in determining the initial target customer and market for IMPULSE. However, it's crucial not to overlook older adults, as they are also embracing digital technology in their quest to participate actively in a digital society (Costa et al., 2019).

Acceptance potential is higher in more sensitive/security-dependent context

The acceptance potential for FRT is notably higher in contexts with heightened security and sensitivity requirements (Krol et al., 2016). Sectors like government, finance, and healthcare, known for their rigorous security requirements and the imperative to protect sensitive data, emerge as promising opportunities for FRT-enabled eID solutions like IMPULSE. In such security/sensitive-dependent contexts, IMPULSE can thrive, ensuring the protection of valuable data assets, streamlining authentication processes, and meeting the escalating demand for advanced identity verification solutions. Furthermore, users are more likely to adopt IMPULSE when they recognize its capacity to reinforce security and preserve sensitive information.

More trust on government and law enforcement agencies

Trust in centralized entities, particularly government and law enforcement agencies, has been relatively well-established in contemporary society (Renduchintala et al., 2022). As FRT gains acceptance, it becomes evident that citizens have greater trust in government and law enforcement entities in contrast to private or commercial companies (Kostka, 2019; Kostka et al., 2023; Ada Lovelace Institute, 2019; Smith, 2019). Furthermore, individuals tend to exhibit a higher comfort level when their biometric data is stored by government institutions rather than private companies (Buckley & Nurse, 2019). Hence, trust in government and law enforcement entities significantly influences the support for FRT adoption (Brewer et al., 2022). This demand, driven by trust, creates an opportunity for FRT-enabled eID solutions like IMPULSE to play a pivotal role in enhancing security and boosting service efficiency across diverse domains. Furthermore, by offering proper service, IMPULSE can build trust with users (Alam et al., 2021).

### 3.4.2 Ecosystem

Ecosystem here refers to the things exists beyond the market, includes such as social/economic/political environment. From an ecosystem standpoint, IMPULSE's opportunities include the possibility of gaining government or company support due to its project origin, as well as consideration of the impact of a pandemic.

Easier to gain government or company support due to originating from a Horizon project

From an ecosystem perspective, IMPULSE stands to gain substantial opportunities, particularly with the potential for government and company support. IMPULSE's roots in a collaborative project supported by the European Commission provide it a distinctive advantage. These collaborative projects are designed to address complicated challenges that require close collaboration among many different stakeholders and prioritize social impacts, value creation, openness, and result also in public benefit. As a result, results of projects like IMPULSE may be seen as more neutral and trustworthy. As a result, IMPULSE is well-positioned to gain governmental and company support, facilitating the successful promotion of IMPULSE within the market.

Pandemic

The COVID-19 pandemic has significantly amplified the demand for digitization and decentralization (Renduchintala et al., 2022). It acted as a catalyst, accelerating the global transition toward secure, contactless digital interactions, underlining the critical importance of robust identity verification. This shift also drove the rapid adoption of remote eHealth solutions (Javed et al., 2021; Whitelaw et al., 2020). With governments, businesses, and individuals soughting ways to minimize physical contact, FRT-enable eID solutions like IMPULSE gained prominence. The opportunities lie in redefining public and private services, particularly in the context of healthcare, remote work, and online transactions. Furthermore, the pandemic has highlighted the importance of robust, scalable, and resilient identity solutions that can adapt to evolving challenges. Notably, the public's willingness to embrace FRT is more pronounced in severe situations where the technology's contactless and convenience benefits are highly valued (Shi et al., 2023). In this context, IMPULSE is well-positioned to address these evolving needs and play a pivotal role in shaping the post-pandemic digital landscape.

## 3.5 Threats for IMPULSE

Threats are '*possible events or forces outside of your control that your company or unit needs to plan for or decide how to mitigate*' (Harvard Business Review, 2005).

The following questions serve as our guidelines for the analysis.

- What are IMPULSE competitors doing?
- What obstacles do IMPULSE face?
- What interesting trends are we aware of?

Threats of IMPULSE can be reflected from the perspectives of competitor, customer, and ecosystem (as shown in Figure 4).


**Figure 4 Threats for IMPULSE**

### 3.5.1 From competitor

Growing number of similar products/services

The growing number of similar products and services provided by various companies competing in the market[29], is a notable threat to IMPULSE. Take Validated ID as an example. A Spanish-based pioneer in decentralized identities with offices in Spain, Germany, France and the UK. They offer a wide range of products such as digital signatures, digital identities and e-invoicing. Their solutions are used in a variety of sectors, including public administration, banking and insurance, and healthcare. Their wallet VIDWallet is an EBSI Compliant advanced SSI-based platform that quickly verifies and manages digital credentials while respecting privacy. A more detailed competitor analysis can be found in D7.14 Exploitation plan V2 to be submitted by the end of the project.

Even more problematic for IMPULSE is that a number of governments have in recent years adopted solutions of their own, for example SPID in Italy. Elsewhere strong incumbents exist, for instance NemID in Denmark. Breaking into markets with strong established players, especially if these are backed by governments, is difficult.

The increasing number of offerings from competitors such as Validated ID or SPID may result in market saturation, intensifying competition, and potentially market share erosion. Moreover, a flood of similar solutions could lead to fragmentation of standards and regulations, raising concerns about interoperability and security. As a result, it is critical for IMPULSE to differentiate itself and stand out in a crowded market by offering tailored solutions to match the individual customer requirements. Addressing this and staying ahead of competitors is vital for the long-term success of IMPULSE.

### 3.5.2 From customer

On the customer side, Threats are most associated with the concerns about the reliability of technology, the privacy of the application, and trust in the service/product provider.

Concern about the reliability of FRT

Users have concerns regarding the reliability of Facial Recognition Technology (FRT), with a particular focus on its accuracy, the possibility of false positives or negatives, and the risk of unauthorized access to personal data or accounts (M.K & Ramayah, 2017; Seng et al., 2021; Shi et al., 2023). As users have been exposed to diverse FRT solutions, they may have negative practical experiences where for instance, children have been unable to unlock a smartphone, or access being granted to the incorrect person, or of key services like online banking being inaccessible in time of need. These concerns can contribute to a lack of trust in FRT, leading to reservations about embracing FRT-enabled eID solutions like IMPULSE.

Low trust to service/product provider

Users are less likely to trust the FRT service providers who are private or commercial companies rather than government or law enforcement entities (Kostka, 2019; Kostka et al., 2023; Ada Lovelace Institute, 2019; Smith, 2019), owing to the assumption that government and law enforcement entities are less likely to misuse personal data (De & Shukla, 2020). To counteract this potential threat, IMPULSE should prioritize transparency, data security, and compliance with privacy regulations. Establishing trust with customers requires clear communication, adherence to ethical data handling practices, and a commitment to customer data protection. Because good customer service can increase trust from customer (Alam et al., 2021), IMPULSE may seek and initial engagement with government and law enforcement entities to launch its

[29] Please refer to D7.14 Exploitation plan V2 for a more detailed analysis of relevant competitors for IMPULSE

adoption and build customer trust. Following that, this trust can be used to expand its further adoption into the private sector.

Concern about privacy violations and the normalisation surveillance

Privacy violation is one of the major concerns associated with the adoption of FRT-enabled systems (Kostka et al., 2021; Krol et al., 2016; Shi et al., 2023). Customers are increasingly concerned about the use of FRT for identity verification. It raises apprehensions regarding extensive data collection, including facial biometrics, and the impact on personal privacy. Furthermore, customers are also concerned about the broader societal impact of normalizing surveillance through the widespread adoption of FRT (Kostka et al., 2021; Ada Lovelace Institute 2019), as the pervasive use of facial recognition in various contexts raises apprehensions about the erosion of civil liberties and the potential creation of a surveillance state.

To address these concerns, in addition to adopt stringent privacy measures, IMPULSE should initiate trust building activities, such as transparently communicating with users and stakeholders about potential privacy impacts, ethical and responsible management of existing risk factors, and the incorporation of adequate safeguards (Beltrán & Calvo, 2023; Casalino et al., 2017). In Belgium, for example, users use an app with access granted exclusively through the National eID Card to check who has accessed their data and for what reason, ensuring exclusive user access – 'only-I-could-use-this' (Sule et al., 2021). Marketing IMPULSE in private sectors should consider the size of the target entities when considering normalisation surveillance. Individuals in smaller businesses, for example, may see the use of an FRT-enabled attendance tracking system as advantageous. However, in larger organizations, some employees may harbor reservations potentially perceiving it as a tool for malicious intent, such as attendance fraud (Otti, 2016).

Not necessary for low-value transactions

Evidence from the literature suggests that deploying FRT-enabled solutions for low-value transactions, such as purchasing a metro ticket or accessing minor online services, is unnecessary, from the users' perspective (Krol et al., 2016). Customers may be resistant or hesitant as a result of this view, as they may regard the usage of FRT for every transaction as excessive and potentially burdensome. As a result, promoting IMPULSE requires careful calibration of its application, reserving its use for scenarios requiring higher security and identity verification. Transparently articulating the benefits and necessity of FRT for specific use cases can help to increase IMPULSE acceptance.

### 3.5.3 From the ecosystem

Regulations, an insufficient range of digitalized/connected public services/systems, and heterogeneous maturity in terms of eID adoption are all potential threats to the adoption of IMPULSE.

Regulations

From an ecosystem standpoint, the evolving and potentially restrictive regulatory requirements linked to eID, particularly FRT-enabled eID, must be considered. While electronic identification guarantees unambiguous identification of a person and ensures the right service is delivered to the right person who is really entitled to it [1], its processing and management at the EU level is governed by principles and norms. With the growing concern about data privacy, security, and potential misuse of FRT, governments and regulatory authorities are considering establishing more strict rules and guidelines.

Compliance with these regulations poses challenges for the commercialization IMPULSE. It will not only raise the complexity and cost of the solution, but also limit the flexibility of IMPULSE in diverse contexts. For example, data protection laws and regulations impede blockchain adoption for FinTech because its 'immutability of recorded transactions' can violate the General Data Protection Regulation (GDPR) under

certain conditions, particularly in terms of the 'right to be forgotten', which gives users the personal right to withdraw and delete transactions and personal information[30]. Furthermore, guidelines published by the Council of Europe [31] and the European Data Protection Board [32] necessitate transparency regarding FRT use by law enforcement. To mitigate this risk, IMPULSE exploitation necessitates proactive adherence to evolving legislation as well as demonstrating a commitment to responsible FRT use. Active interaction with regulators, industry groups, and standards bodies, for example, is suggested to help shape regulations that balance the benefits of IMPULSE with privacy and security concerns. [33]

Insufficient range of digitalized/connected public services/systems

According to the literature[34] and the findings of the IMPULSE pilot case, the existing range of digitalized and connected public services/systems is insufficient to support widespread adoption of IMPULSE in e-government alone. The availability and integration of digital services provided by governments and private entities is critical to the effectiveness of eID solutions, such as IMPULSE. If the digital infrastructure is not sufficiently developed or lacks connectivity, the utility and adoption of IMPULSE will be severely limited. Practically this could mean that only a fraction of services or systems can be accessed, or economic or societal gains are barely anticipated. Moreover, incomplete integration might lead to fragmented user experiences and impede the seamless access to diverse services.

Heterogenous maturity in respect to eID adoption

Both the literature and the IMPULSE pilot cases reflected the various maturity level of eID adoption among countries (Kostka et al., 2021), which will have an impact on IMPULSE marketing. Governments, industries, and user populations vary in their readiness and willingness to adopt eID solutions, particularly those enabled by FRT, which can pose challenges for the seamless implementation and integration of IMPULSE. If the target entities are in a situation/region where eID adoption is still in its early stages, they may be hesitant to adopt IMPULSE, especially as it is enabled by FRT. People who have used FRT in real life (e.g., unlocking personal devices) will find it more useful and be more willing to use it in another context, in contrast to those who lack prior exposure to FRT (Seng et al., 2021).

[30] https://gdpr-info.eu/issues/right-to-be-forgotten/, Right to be Forgotten
[31] https://rm.coe.int/guidelineson-facial-recognition/1680a134f3, Guidelines on Facial Recognition
[32] https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 1
[33] More details on the analysis of relevant standards, legal and ethical implications see Deliverables 3.1 – 3.7.
[34] https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2023, eGovernment benchmark 2023

## 3.6 Summary of SWOT analysis

To summarize, the SWOT analysis result is presented in Figure 5.

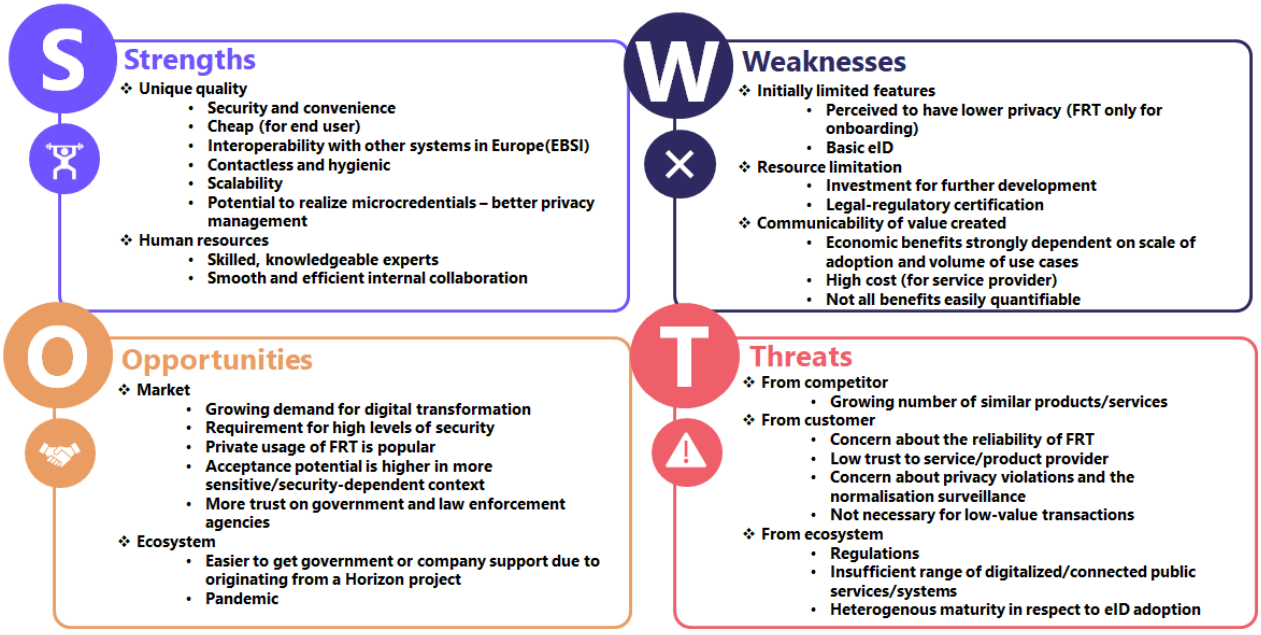


**Figure 5 Summary of SWOT analysis for IMPULSE eID solution**

Considering the results of the SWOT analysis, promoting IMPULSE adoption should begin with commercializing basic, fast and simple eID offerings, progressing to advanced eID functionality. It is critical to establish trust through early adopters from the public and/or private sectors. Meanwhile, as learned from COVID-19, opportunistic exploitation possibilities should be examined. Finally, the micro-credentials realized by IMPULSE have the potential to offer unique and novel business models. Following are more comprehensive recommendations for the practical implementation of IMPULSE.

1. **Ensuring the existence of sufficient number of valuable and/or high-volume-of-usage use cases** (services to be accessed) that eID can be used on. People are unlikely to adopt eIDs if their applicability is limited to a few scenarios or sporadic needs. Therefore, in practice, collaborating with the private sector from the outset, or at least from an early stage, is essential to assure an adequate volume of private sector use cases. The reason for this is that people generally use private-sector use cases more intensively in their daily lives compared to public sector use cases. For instance, studies such as Initiative D-21 "E-Government Monitor" surveys (annual, representative survey of the DACH-region)[35] have revealed that people typically use no more than 3-5 public services per year. Few people will acquire an eID only to facilitate access to these infrequently used services. In contrast, online banking, a private sector use case, is frequently used daily. In this context, the provision of a legally valid signature capability by the eID solution holds particular significance, as it unlocks numerous high-value use cases (services), reinforcing the overall appeal and utility of the eID solution. However, it should be noted that IMPULSE currently cannot offer the legally valid signature capability.

2. **Ensuring high usability of the eID solution** as well as the **registration process** for obtaining it. The significance of the solution's usability is evident and probably requires little further elaboration. Systems that are cumbersome to use, require additional hardware or components, or are expensive are unlikely to gain widespread acceptance. But perhaps equally crucial is the registration process. eIDs that require lengthy visits to public offices, necessitate additional documents/letters/log-ins, and so on

[35] https://initiatived21.de/publikationen/egovernment-monitor

will likely to attract fewer users than eIDs that keep the number and complexity of the steps in the registration process as few and simple as possible. For instance, instead of making the eID an additional, optional thing that requires a separate opt-in, it may be issued automatically as part of processes like passport/ID card renewal (possibly with an opt-out option for legal reasons), rather than making the eID an additional, optional thing that requires a further opt-in. The case of Germany exemplifies the long time impact of complex/cumbersome registration processes (opt-in with additional steps, rather than opt-out with few or no additional steps) on hindering the widespread adoption of eIDs.

3. **Appropriate state regulation**. The government can take various measures make eID adoption more appealing. This can include subsidies (e.g., Estonia subsidized digital signatures, where citizens get a specific number of signatures for free each year), but it can also include, and perhaps especially, regulation of how state agencies approach digitization. Key rules include, for examples, Estonia's "Once-Only" principle, stipulating that data digitally submitted by citizens once, to one state agency, cannot be subsequently requested again by another state agency. Rather, the agencies are mandated to share the data with each other (subject to data protection rules such as legitimate ground for processing) so that citizens do not need to submit it multiple times. This practice not only streamlines digital processes but also makes using digital process (and thus eIDs) more attractive for citizens. A further sensible regulation (and technical architecture) is 'transparency portals', which allow citizens to know at all times which state agencies are use what data of theirs for which purposes, such as the app in Belgium. This provides citizens greater levels of transparency than analog, paper-based processes would, and can thus help foster public acceptance for eIDs.

4. **Reach an agreement** with key stakeholders **on a single eID solution**, and then stick to it, focus resources on it and implement it. One widely implemented and used solution outperforms multiple solutions that are only infrequently implemented or used. Given the rapid pace of technical change, there is a risk that, in the absence of sufficient coordination between government ministries and/or key stakeholders, numerous actors begin implementing or experimenting with their own proprietary or experimental eID solution. This is liable to create a fragmented eID landscape where many solutions and services are *not* interoperable and adoption is thus slow, but actors from business and technology have also shouldered too large sunk costs to be willing to discontinue their proprietary solutions in favour of a new, common one. Germany is arguably an example of this. A better approach would be to reach agreement among all the main actors on one single solution and then stick to this.

5. **Exploit (technological) windows of opportunity**. The cost (friction) of switching from one (e)ID system to another is relatively high for users. Even if a given eID system has disadvantages, users will not automatically migrate to a better one. This is a serious concern for 2nd, 3rd of 4th generation eID systems like IMPULSE, where existing users already have an eID system face considerable barriers to switching to a new one, even if they agree that the new one is objectively better. Public and private actors who want to push a new eID system should therefore look for windows of opportunity, occasions when these barriers are lowered, and strategically push the new system at those moments. One example is when people need to renew their ID cards or other crucial documents, or when they are registering for a new and important service (for example, bank accounts or credit cards). During these instances, they already have to go through a number of bureaucratic steps and processes, and adding a further one (e.g., to register for the new eID system) adds comparatively less burden. Moreover, there may be synergies in the registration processes, further reducing burdens on users. Another example is the broad adoption of FRT-enabled identification apps during COVID-19 (Shi et al., 2023), where the benefits of adoption, such as contactless, hygiene, and efficiency, outweigh the cost associated with the registration process or the lack of trust in the technology.

6. **Systematic and substantial education/information campaigns** to popularise the new eID system and raise citizens awareness of their benefits and the services that can be accessed through them.

Estonia's successful experience in transitioning to digital government (which in turn depends on people having and using eIDs), suggests that such campaigns seem to have played a significant role. By effectively communicating the value proposition of the new eID system and illustrating the spectrum of services it enables, these initiatives can contribute significantly to fostering public acceptance and engagement. Essentially, the IMPULSE project itself has immense educational potential, particularly in terms of explaining and promoting the adoption of the new eID system as it raises individuals' awareness of its advantages. For example, the increased security and time savings. Furthermore, the IMPULSE project offers a unique opportunity to delve into the spectrum of services enabled by the new eID system, such as easy access to governmental services, streamlined administrative processes to access law enforcement agencies, and FRT-enabled lockers for homeless shelter residents. Therefore, the project has the potential to transform the perception of the eID system from a novel technological advancement to an indispensable tool that enhances residents' daily lives, not only raising awareness but also empowering individuals with the knowledge needed to make informed decisions about its adoption.

# 4 Business model options

A business model is a description of the key principles that govern how an organization creates, delivers, and captures value (Osterwalder & Pigneur, 2010). It covers the fundamentals of the business, such as the value proposition, cost structure, and revenue streams. Furthermore, it provides information about target customer segments, distribution channels, key partners, resources, and activities. Typically, business models serve as a framework to describe the business, yet they can also function as a management tool to guide future development.

In practice, the development of business model involves developing an understanding of customer needs and describing how to meet these needs or address their problems. Central to the business model is value proposition, which describe the benefits and value of the solution from the perspective of the customers and users. The other elements of the model focus on describing how this value is delivered, including the cost structure and revenue streams. All the elements are inextricably linked to the value proposition. Among other things, the building blocks outlined in the Business Model Canvas (Osterwalder & Pigneur, 2010) are used in this report to assist in the development of the IMPULSE business model.

Various business model options come with different requirements and are suitable for varying time scales. To mitigate the weakness of individual business models and facilitate the long-term exploitation and commercialization of IMPULSE, four prototypical business models operating on different time scales (i.e., short-term and long-run) and focusing on different customer segments (i.e., public sectors and private sectors) are proposed, as illustrated in Figure 6. It is important to note that these are B2B models proposed from the perspective of IMPULSE, and the end users will be determined by the customer segments in these models. End users often expect (and enjoy) free services, while other ecosystem participants pay for the custom features or cost efficiency in their processes enabled by the solution. These recommended business model options are presented in the format of Business Model Canvas in the subsequent subsections.

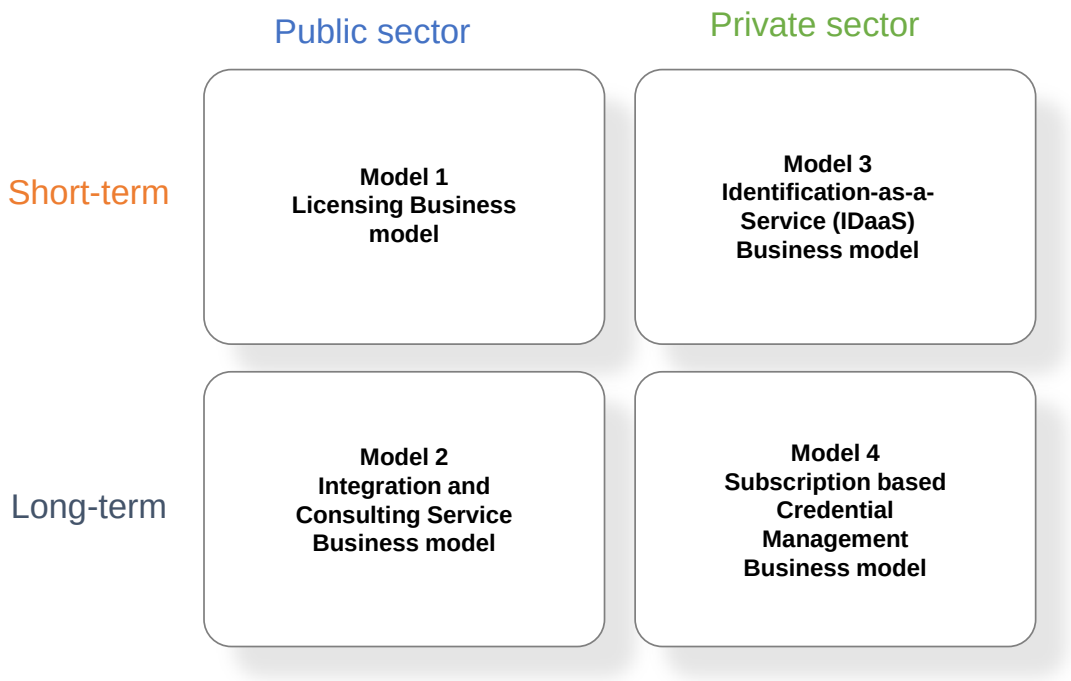


**Figure 6 Summary of Business Model options**

## 4.1 Business model options in public sector

### 4.1.1 Model 1 (short-term): Licensing business model

The first business model proposed for the public sector is Model 1, *Licensing business model*, as shown in Figure 7. It is a short-term business model that is based on licensing the IMPULSE technologies with limited customization and integration services. IMPULSE, as an FRT-enabled eID solution, had gone through pilot cases in different countries for diverse objectives. Because it is still a basic eID solution, the short-term business model is designed to meet customer needs while minimizing the investment from IMPULSE's side.

Licensing can be an appropriate and effective business model in the public sector, offering cost-effective and efficient solutions to public sector entities such as government agencies. Technology licensing offers government agencies the opportunity to license IMPULSE, thus transferring technology and enabling secure identity verification and access control for public services. When compared to developing similar solution in-house, it provides government agencies with an efficient approach to implement new eID solutions like IMPULSE without incurring significant development costs. Furthermore, IMPULSE can tailor its technology to meet the specific demands of government agencies, providing customized solutions that seamlessly integrate with their existing infrastructure. Therefore, in the public sector, licensing can be a mutually beneficial approach for IMPULSE and government agencies. It enables the government agencies to access advanced technology without lock-ins to costly service agreements, or incurring the entire development cost and offers IMPULSE with a revenue stream while expanding its reach in the public sector. It allows for adaptability to specific government needs while adhering to regulatory requirements. The key principles behind this archetype are to seek minimal cost of operating the model, and to effectively leverage the potential to learn from the implementations to support the further development of IMPULSE features and long-term business.

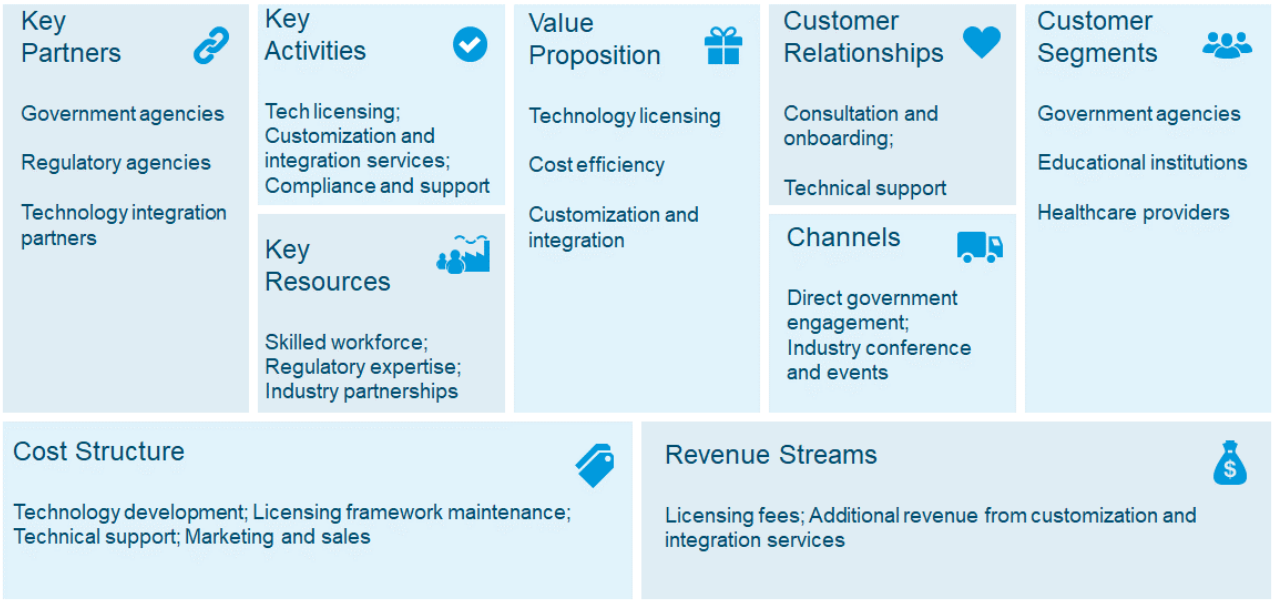


**Figure 7 Model 1 (short-term): Licensing business model**

### 4.1.2 Model 2 (long-term): Integration and Consulting Service business model

Model 2, *Integration and Consulting Service business model*, is the second business model advised for the public sector, as depicted in Figure 8. It is a long-term business model that is built around integration and consulting services. Given IMPULSE's potential to integrate microcredentials, Model 2 provides public sector entities with the expertise, support, and customization required to successfully implement and manage electronic identification and microcredentialing systems. This model offers a variety of services to ensure that IMPULSE aligns with the unique needs and requirements of the specific agency. At the same time, it can streamline the integration process to reduce disruptions and enhance efficiency. As opposed to the short-term model, this archetype is focused on the unique value proposition and close, collaborative customer relationship that allow IMPULSE to fully leverage its both its technical features and the strong expertise behind it.


**Figure 8 Model 2 (long run): Integration and Consulting Service business model**

## 4.2 Business model options in private sector

### 4.2.1 Model 3 (short-term): Identification-as-a-Service (IDaaS) business model

Model 3, *Identification-as-a-Service (IDaaS) business model*, is the short-term business model targeted to the private sector, as shown in Figure 9. This model focuses on the existing functionalities of IMPULSE, similar to the justification for the short-term model in the public sector. This model provides private sector clients with customized FRT-enabled eID solutions that are tailored to their specific requirements. In addition, the customized IMPULSE may develop with the business and adapt to its evolving requirements, i.e., scalability. It will ensure that the customized solution adheres to industry regulations and compliance standard because it provides an Identification-as-a-Service (IDaaS) bundle to customers. Customization fees, maintenance and support fees, and integration fees can all generate revenue. In this model, the essential value of IMPULSE to the customer segments comes from offering an easy, yet customizable and expandable option for addressing the customer's identity management needs with a low-risk subscription and extra fees payment model.


**Figure 9 Model 3 (short-term): Identification-as-a-Service (IDaaS) business model**

### 4.2.2 Model 4 (long-term): Subscription based Credential Management business model

Model 4, *Subscription based Credential Management business model*, is the second business model proposed for the private sector, as shown in Figure 10. It is a long-term business model that provides a comprehensive platform for managing electronic identities and microcredentials to private-sector enterprise through a subscription-based service. This model allows clients to access, customize, and maintain their eID and microcredential systems without making substantial upfront investments. It is a scalable solution allowing private-sector enterprises to issue, manage, and verify microcredentials for their employees, clients, or members. It ensures a seamless and secure experience with an affordable, predictable cost structure through subscription pricing, reducing the need for substantial capital expenditures.

This archetype operates as a platform business model. Wherein the previous short term model IMPULSE manages the identity needs on behalf of the client, in the platform model here it offers open tools, policies and a platform for the different actors on the multi-sided market - the issuers, users, managers and developers of eID services. This enables the different parties to form a platform-based ecosystem, where eID innovation and adoption may take place facilitated by the IMPULSE platform that offers coordination, governance and assures the adherence to regulations and standards.

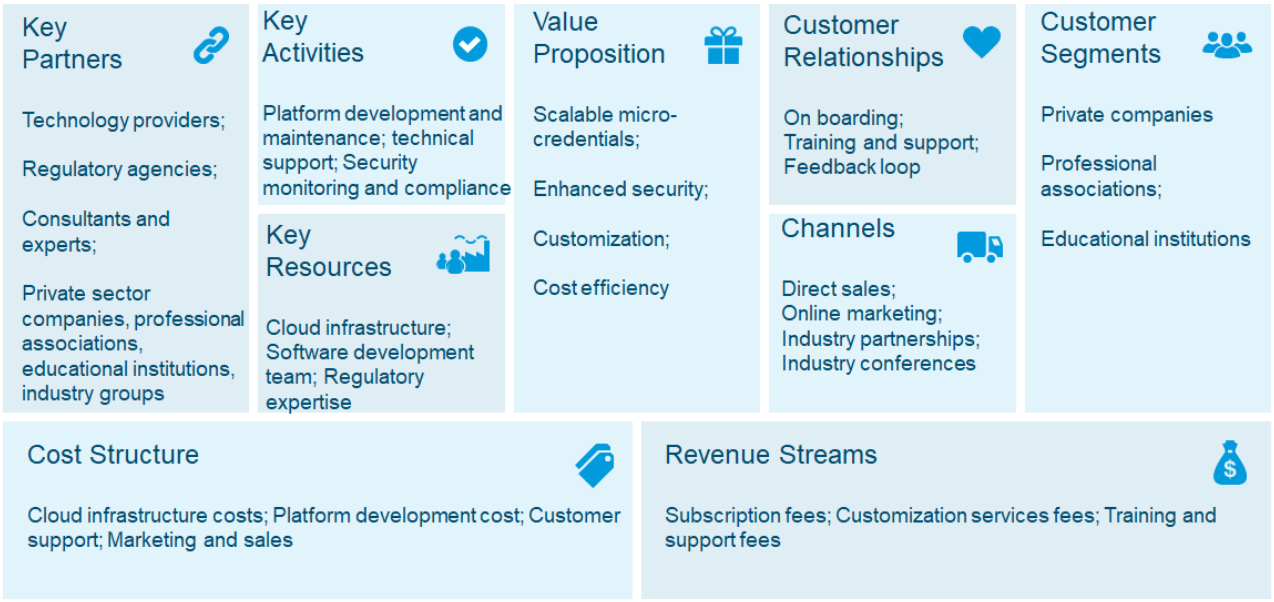


**Figure 10 Model 4 (long-term): Subscription based Credential Management business model**

# 5 Conclusion

IMPULSE eID solution has the potential to be used in both the public and private sectors with a variety of business model options, provided that its strengths are taken into consideration, its opportunities are maximized, and the threats are minimized. The unique features of IMPULSE and the partners behind its creation enable the pursuit of short-term exploitation of project results through licensing and service business models that maximize learning opportunities and resource availability for the IMPULSE development while providing easy implementation to customers. Given sufficient development and favourable market conditions the long-term business models of IMPULSE could scale the business both for deeper and broader customer engagement over consulting and platform models.

# References


Abdul, W., Alzamil, A., Masri, H., ul Haq, Q. E., Ghouzali, S., Hussain, M., & AlZuair, M. (2017). Fingerprint and Iris Template Protection for Health Information System Access and Security. *Journal of Medical Imaging and Health Informatics*, *7*(6), 1302–1308. https://doi.org/10.1166/jmihi.2017.2149

Ada Lovelace Institute (2019). Beyond face value: public attitudes to facial recognition technology, https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/, accessed 19.05.2023.

Alam, Md. M., Awawdeh, A. E., & Muhamad, A. I. Bin. (2021). Using e-wallet for business process development: challenges and prospects in Malaysia. *Business Process Management Journal*, *27*(4), 1142–1162. https://doi.org/10.1108/BPMJ-11-2020-0528

Alzaabi, M., Almeheiri, M., Alqubaisi, S., & Shuhaiber, A. (2023). "AI-Teacher" Assistant System: A Smart Attendance and Participation tracking system for students. *2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023*. https://doi.org/10.1109/SmartNets58706.2023.10215586

Baby Shamini, P., Sujay Nithish, H., & Surendar, N. (2022). Bank Transaction using Face Recognition. *International Interdisciplinary Humanitarian Conference for Sustainability, IIHC 2022 - Proceedings*, 772–774. https://doi.org/10.1109/IIHC55949.2022.10060800

Beltrán, M., & Calvo, M. (2023). A privacy threat model for identity verification based on facial recognition. *Computers and Security*, *132*. https://doi.org/10.1016/j.cose.2023.103324

Brewer, P. R., Bingaman, J., Dawson, W., Paintsil, A., & Wilson, D. C. (2022). Eyes on the Streets: Media Use and Public Opinion About Facial Recognition Technology. *Bulletin of Science, Technology and Society*, *42*(4), 133–143. https://doi.org/10.1177/02704676221148103

Buckley, O., & Nurse, J. R. C. (2019). The language of biometrics: Analysing public perceptions. *Journal of Information Security and Applications*, *47*, 112–119. https://doi.org/10.1016/j.jisa.2019.05.001

Bull, J. W., Jobstvogt, N., Böhnke-Henrichs, A., Mascarenhas, A., Sitas, N., Baulcomb, C., Lambini, C. K., Rawlins, M., Baral, H., Zähringer, J., Carter-Silk, E., Balzan, M. V., Kenter, J. O., Häyhä, T., Petz, K., & Koss, R. (2016). Strengths, Weaknesses, Opportunities and Threats: A SWOT analysis of the ecosystem services framework. *Ecosystem Services*, *17*, 99–111. https://doi.org/10.1016/j.ecoser.2015.11.012

Carlos-Roca, L. R., Torres, I. H., & Tena, C. F. (2018). Facial recognition application for border control. *2018 International Joint Conference on Neural Networks (IJCNN)*, 1–7. https://doi.org/10.1109/IJCNN.2018.8489113

Casalino, N., Ciarlo, M., Sassetti, S., & Panico, M. (2017). Management and innovation models for Digital Identity in public sector. *ICEIS 2017 - Proceedings of the 19th International Conference on Enterprise Information Systems*, *1*, 225–232. https://doi.org/10.5220/0006279202250232

Chadwick, D. W., Laborde, R., Oglaza, A., Venant, R., Wazan, S., & Nijjar, M. (2019). Improved Identity Management with Verifiable Credentials and FIDO. *IEEE Communications Standards Magazine*, *3*(4), 14–20. https://doi.org/10.1109/MCOMSTD.001.1900020

Chermack, T. J., & Kasshanna, B. K. (2007). The use and misuse of swot analysis and implications for hrd professionals. *Human Resource Development International*, *10*(4), 383–399. https://doi.org/10.1080/13678860701718760

Costa, C., Gilliland, G., & McWatt, J. (2019). 'I want to keep up with the younger generation' - older adults and the web: a generational divide or generational collide? *International Journal of Lifelong Education*, *38*(5), 566–578. https://doi.org/10.1080/02601370.2019.1678689

Da Costa Rocha, J., De Souza, M. A., Cardoso, E. H. S., Vijaykumar, N., De Araujo, J. P. L., & Frances, R. L. (2023). A Platform for Monitoring Student Commuting in the Use of School Transport in Smart Cities - A Facial Recognition Based Approach. *2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023*. https://doi.org/10.1109/SmartNets58706.2023.10216190

De, S. J., & Shukla, R. (2020). Privacy policies of e-governance initiatives: Evidence from India. *Journal of Public Affairs*, *20*(4). https://doi.org/10.1002/pa.2160

Echikson, William (2020): Europe's Digital Identifcation Opportunity. The Centre for European Policy Studies (CEPS), https://www.ceps.eu/wp-content/uploads/2020/06/TFR_Europe-Digital-Identification-Opportunity. Accessed 08.08.2023.

Eneman, M., Ljungberg, J., Raviola, E., & Rolandsson, B. (2022). The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities. *Information Polity*, *27*(2), 219–232. https://doi.org/10.3233/IP-211538

European Commission. (2020). The Commission has launched a public consultation on the revision of the rules on electronic identification and trust services for electronic transactions in the internal market, the eIDAS Regulation, available at https://ec.europa.eu/digital-single-market/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation. Accessed 22.06.2023.

European Commission. (2021). Study to support the impact assessment for the revision of the eIDAS regulation, available at https://op.europa.eu/en/publication-detail/-/publication/9ce0f9e5-03bb-11ec-8f47-01aa75ed71a1/language-en/format-PDF/source-225913375. Accessed 08.08.2023.

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00620-z

Harvard Business Review. (2005). *Strategy: Create and Implement the Best Strategy for Your Business*. Harvard Business School Press.

Hill, T., & Westbrook, R. (1997). SWOT analysis: It's time for a product recall. *Long Range Planning*, *30*(1), 46–52. https://doi.org/10.1016/S0024-6301(96)00095-7

Hoskisson, R. (1999). Theory and research in strategic management: swings of a pendulum. *Journal of Management*, *25*(3), 417–456. https://doi.org/10.1016/S0149-2063(99)00008-2

Hsu, C. S., Tu, S. F., & Chiu, P. C. (2022). Design of an e-diploma system based on consortium blockchain and facial recognition. *Education and Information Technologies*, *27*(4), 5495–5519. https://doi.org/10.1007/s10639-021-10840-5

Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., & Qureshi, K. N. (2021). Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. *Healthcare*, *9*(6), 712. https://doi.org/10.3390/healthcare9060712

Jayakumar, K., Surendar, V., Sheela, A., Javagar, P., Riyas, K. A., & Dhanush, K. (2022). Internet of Things based Biometric Smart Attendance System. *International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2022 - Proceedings*, 1492–1497. https://doi.org/10.1109/ICSCDS53736.2022.9761045

Koonin, L. M., Hoots, B., Tsang, C. A., Leroy, Z., Farris, K., Jolly, B., Antall, P., McCabe, B., Zelis, C. B. R., Tong, I., & Harris, A. M. (2020). Trends in the Use of Telehealth During the Emergence of the COVID-19 Pandemic — United States, January–March 2020. *MMWR. Morbidity and Mortality Weekly Report*, *69*(43), 1595–1599. https://doi.org/10.15585/mmwr.mm6943a3

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, *21*(7), 1565–1593. https://doi.org/10.1177/1461444819826402

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, *30*(6), 671–690. https://doi.org/10.1177/09636625211001555

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, *40*(1). https://doi.org/10.1016/j.giq.2022.101761

Krol, K., Parkin, S., & Sasse, M. A. (2016). "I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement. *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, 1–7. https://doi.org/10.1109/ISBA.2016.7477235

Lin, J. Da, Lin, H. H., Dy, J., Chen, J. C., Tanveer, M., Razzak, I., & Hua, K. L. (2022). Lightweight Face Anti-Spoofing Network for Telehealth Applications. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1987–1996. https://doi.org/10.1109/JBHI.2021.3107735

Martin, N. 2023: "The Chimera of Control. Some Critical Reflections on Self-Sovereign Identity". Paper presented at the fifteenth interdisciplinary workshop on "Privacy, Data Protection & Surveillance", 18 July 2023, Alexander von Humboldt Institute for Internet and Society, Berlin

Martinez-Martin, N. (2019). What are important ethical implications of using facial recognition technology in health care? *AMA Journal of Ethics*, *21*(2), 180–187. https://doi.org/10.1001/amajethics.2019.180

Matulionyte, R. (2023). Increasing transparency around facial recognition technologies in law enforcement: towards a model framework. *Information and Communications Technology Law*. https://doi.org/10.1080/13600834.2023.2249781

M.K, N., & Ramayah, T. (2017). Trust in Internet Banking in Malaysia and the Moderating Influence of Perceived Effectiveness of Biometrics Technology on Perceived Privacy and Security. *Journal of Management Sciences*, *4*(1), 3–26. https://doi.org/10.20547/jms.2014.1704101

NEC Corporation (2020). NEC to provide facial recognition technology for Mitsui Fudosan hotels - "Smart Hospitality Service" for "Sequence" brand hotels. https://www.nec.com/en/press/202001/global_20200128_01.html, accessed 10.11.2023

North-Samardzic, A. (2020). Biometric Technology and Ethics: Beyond Security Applications. In *Journal of Business Ethics* (Vol. 167, Issue 3, pp. 433–450). Springer Science and Business Media B.V. https://doi.org/10.1007/s10551-019-04143-6

OECD (2023). Micro-credentials for Lifelong Learning and Employability: Uses and Possibilities, OECD Education Policy Perspectives, No. 66, OECD Publishing, Paris. https://doi.org/10.1787/9c4b7b68-en, accessed 25.9.2023

Osterwalder, A., & Pigneur, Y. (2010). *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. Johan Wiley & Sons.

Otti, C. (2016). Comparison of biometric identification methods. *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 339–344. https://doi.org/10.1109/SACI.2016.7507397

Rachel, S. S., P, P. K., & B, Y. K. (2022). Edsys: A Smart Campus Management System. *2022 1st International Conference on Computational Science and Technology (ICCST)*, 726–730. https://doi.org/10.1109/ICCST55948.2022.10040436

Renduchintala, T., Alfauri, H., Yang, Z., Pietro, R. Di, & Jain, R. (2022). A Survey of Blockchain Applications in the FinTech Sector. In *Journal of Open Innovation: Technology, Market, and Complexity* (Vol. 8, Issue 4). MDPI. https://doi.org/10.3390/joitmc8040185

Richter, D., & Anke, J. (2021). Exploring Potential Impacts of Self-Sovereign Identity on Smart Service Systems An Analysis of Electric Vehicle Charging Services. *Business Information Systems*, *1*, 105–116. https://doi.org/10.52825/bis.v1i.68

Sara Philomin, V., Srinivasulu, S., Abirami, M., Raj, J. R., Jabez, J., & Gowri, S. (2022). A Contemporary Cloud-based Dynamic Authentication System for Mobile Applications. *International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2022 - Proceedings*, 1259–1265. https://doi.org/10.1109/ICSCDS53736.2022.9760937

Seng, S., Al-Ameen, M. N., & Wright, M. (2021). A first look into users' perceptions of facial recognition in the physical world. *Computers & Security*, *105*, 102227. https://doi.org/10.1016/j.cose.2021.102227

Sharma, S., Saini, A., & Chaudhury, S. (2023). A survey on biometric cryptosystems and their applications. In *Computers and Security* (Vol. 134). Elsevier Ltd. https://doi.org/10.1016/j.cose.2023.103458

Shi, J., Hu, X., & Guo, X. (2023). The lesser of two evils: Assessing the public acceptance of AI thermal facial recognition during the COVID-19 crisis. *Risk Analysis*. https://doi.org/10.1111/risa.14198

Simões, R. B., Amaral, I., Flores, A. M. M., & Antunes, E. (2023). Scripted Gender Practices: Young Adults' Social Media App Uses in Portugal. *Social Media and Society*, *9*(3). https://doi.org/10.1177/20563051231196561

Smith, A. (2019). More than half of U.S. adults trust law enforcement to use facial recognition responsibly. Pew Research Center. September 5 https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facialrecognition-responsibly/, accessed 08.08.2023.

Statista. (2023). Number of mobile app downloads worldwide from 2016 to 2022(in)billions. www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads, accessed 08.08.2023.

Sukmandhani, A. A., & Sutedja, I. (2019). Face Recognition Method for Online Exams. *2019 International Conference on Information Management and Technology (ICIMTech)*, 175–179. https://doi.org/10.1109/ICIMTech.2019.8843831

Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. *Technology in Society*, *67*. https://doi.org/10.1016/j.techsoc.2021.101734

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law and Security Review*, *33*(4), 470–481. https://doi.org/10.1016/j.clsr.2017.03.016

Toth, K. C., & Anderson-Priddy, A. (2019). Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Security & Privacy*, *17*(3), 17–27. https://doi.org/10.1109/MSEC.2018.2888782

Valentin, E. K. (2001). Swot Analysis from a Resource-Based View. *Journal of Marketing Theory and Practice*, *9*(2), 54–69.

Wang, J. S. (2021). Exploring biometric identification in FinTech applications based on the modified TAM. *Financial Innovation*, *7*(1). https://doi.org/10.1186/s40854-021-00260-2

Weihrich, H. (1982). The TOWS matrix—A tool for situational analysis. *Long Range Planning*, *15*(2), 54–66. https://doi.org/10.1016/0024-6301(82)90120-0

White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M. and Sperling, O. (2019): Digital identification: A key to inclusive growth. McKinsey & Company, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx, accessed 08.08.2023

Whitelaw, S., Mamas, M. A., Topol, E., & Van Spall, H. G. C. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, *2*(8), e435–e440. https://doi.org/10.1016/S2589-7500(20)30142-4

Zhang, J., Calabrese, C., Ding, J., Liu, M., & Zhang, B. (2018). Advantages and challenges in using mobile apps for field experiments: A systematic review and a case study. *Mobile Media & Communication*, *6*(2), 179–196. https://doi.org/10.1177/2050157917725550

Zhang, L. L., & Kim, H. K. (2021). The impacts of customer characteristics on innovation resistance in using face recognition payment systems: An empirical study. *Journal of System and Management Sciences*, *11*(3), 101–118. https://doi.org/10.33168/JSMS.2021.0306

# Annex A Business Model Canvas description for Model 1

**Model 1: Licensing business model (public sector, short-term)**

***Value Propositions*:**

- **Technology licensing**: offers government agencies the opportunity to license IMPULSE, thus transferring technology, ensuring secure identity verification and access control for public services.
- **Cost Efficiency**: Cost savings to government agencies compared to building similar solution in-house. It offers an efficient way to adopt FRT-based eID solutions like IMPULSE without significant development costs.
- **Customization and integration**: IMPULSE can tailor its technology to suit the specific needs of government agencies, providing customized solutions that integrate seamlessly with existing infrastructure.

***Key Partners***

- **Government agencies**: should establish partnerships with government agencies at various levels (local, regional, and national) interested in adopting IMPULSE.
- **Regulatory agencies**: Collaborate with regulatory authorities to ensure compliance with data privacy and security regulations.
- **Technology integration partners**: Partner with firms or organizations specializing in integrating licensed technology into existing government systems.

***Key Activities:***

- **Technology licensing**: Develop a clear licensing framework, specifying the terms, conditions, and pricing for government agencies to adopt IMPULSE.
- **Customization and Integration Services**: Offer expertise in customizing and integrating the licensed technology to meet specific government requirements.
- **Compliance and support**: Ensure that the IMPULSEs solution adheres to all relevant data security and privacy regulations and provide ongoing support and updates.

***Key resources***

- **Skilled workforce**: Skilled engineers and software developers to maintain and improve the system.
- **Regulatory expertise**: In-depth knowledge of legal and privacy regulations related to identity verification in the public sector
- **Industry partnerships**: Establish strong connections with technology providers, legal experts, and compliance specialists.

***Customer Relationships*:**

- **Consultation and onboarding**: Develop strong relationships through consultation during the licensing process and onboarding to ensure a seamless transition.
- **Technical support**: Provide ongoing technical support to assist government agencies in implementing and maintaining the licensed IMPULSE

***Channels*:**

- **Direct government engagement**: Reach out to government agencies at various levels through direct communication and presentations.
- **Conferences and events in public sector and industry**: Participate in events and conferences in public sector and industry to showcase the licensing opportunities.

***Customer Segments*:**

- **Government agencies**: Target government agencies, municipalities, and public services that require secure identity verification and access control.
- **Educational institutions**: Focus on schools, universities, and training centers looking to manage digital student and staff identities
- **Healthcare providers**: Serve healthcare organizations requiring secure patient and staff identification.

***Cost Structure*:**

- **Technology development**: Costs related to developing, maintaining, and customizing IMPULSE for government clients.
- **Licensing framework maintenance**: Legal and administrative costs associated with maintaining licensing agreements.
- **Technical support**: Investment in a support team to provide technical assistance to government clients.
- **Marketing and sales**

***Revenue Streams*:**

- **Licensing Fees**: IMPULSE Generates revenue through licensing fees paid by government agencies for the use of its technology.
- **Customization and Integration Services**: Additional revenue can be earned through customization and integration services provided to tailor IMPULSE for specific use cases.

# Annex B Business Model Canvas description for Model 2

**Model 2: Integration and Consulting Service Business model (public sector, long-term)**

***Value Propositions:***

- **Expertise**: Offer extensive knowledge and experience in electronic identification, microcredentials, and secure identity management.
- **Customization**: Tailor eID solutions to the specific needs and processes of government agencies.
- **Efficiency**: Streamline the integration process to minimize disruptions and maximize efficiency.

***Key Partners:***

- **Government agencies**: Establish partnerships with government entities at various levels (local, regional, national) to provide eID and micro-credentialing services.
- **Technology providers**: Collaborate with technology providers for hardware, software, and security solutions.
- **Legal and compliance experts**: Partner with legal and compliance professionals to ensure adherence to data protection and security regulation

***Key Activities:***

- **Analysis and assessment**: Conduct in-depth assessment of the agency's existing systems and needs to determine the best approach.
- **Customization and integration**: Customize IMPULSE to meet agency requirements and integrate it with existing systems.
- **Training and support**: Provide training and ongoing support to agency staff for system operation and maintenance.
- **Security and compliance**: Ensure that IMPULSE meets security standards and complies with data protection regulations.

***Key Resources:***

- **Skilled Workforce**: Employ experts in eID, micro-credentials, system integration, and security.
- **Technology**: Access to cutting-edge technology, including secure authentication methods and encryption protocols.
- **Industry partnerships**: Establish strong connections with technology providers, legal experts, and compliance specialists.

***Customer Relationships:***

- **Consultation**: Maintain an ongoing consultancy relationship with government agencies to understand their evolving needs.
- **Training and support**: Offer training sessions, user support, and troubleshooting to ensure the smooth operation of the eID system.
- **Feedback and improvement**: Gather feedback from agencies to continuously enhance IMPULSE.

***Channels:***

- **Direct sales**: Engage in direct sales and marketing efforts to government agencies to promote integration and consulting services.
- **Online platforms**: Utilize digital channels, such as a professional website, to provide information and engage with potential clients.

- **Industry conferences**: Attend and participate in industry conferences to network and showcase expertise.

***Customer Segments**:*

- **Government agencies**: The primary customer segment includes local, regional, and national government entities seeking eID solutions.
- **Healthcare and Education**: Subsegments may include healthcare providers, educational institutions, and other public organizations with specific eID and micro-credentialing needs.

***Cost Structure**:*

- **Human Resources**: The major cost includes salaries and benefits for skilled staff.
- **Technology infrastructure**: Expenses related to maintaining secure infrastructure for IMPULSE.
- **Marketing and sales**: Costs associated with marketing efforts and sales activities.
- **Training and support**: Investment in training resources and customer support.

***Revenue Stream**:*

- **Consulting fees**: Charge fees for consultancy, assessment, customization, and integration services.
- **Licensing and maintenance**: Generate ongoing revenue through licensing agreements and maintenance contracts.
- **Training and support fees**: Offer training and support packages with associated fees.
- **Customization and integration charges**: Bill for customization and integration work based on the complexity of the project.

# Annex C Business Model Canvas description for Model 3

**Model 3: Identification-as-a-Service (IDaaS) Business model (private sector, short-term)**

***Value Propositions:***

- **Tailored solutions**: Offer custom FRT-based eID solutions for private sector clients to meet their unique needs.
- **Scalability**: The tailored IMPULSE can scale with business growth and evolving requirements.
- **Compliance assistance**: Ensure clients' solutions adhere to industry regulations and compliance standards.

***Key Partners:***

- **Private sector businesses**: Collaborate closely with businesses seeking personalized identity solutions.
- **FRT providers**: Partner with FRT technology companies for specialized technology.
- **DLT providers**: Partner with DLT companies for specialize technology
- **Regulatory agencies**: Collaborate with regulatory authorities to ensure compliance with data privacy and security regulations.

***Key Activities:***

- **Solution development**: Create customized identity verification solutions tailored to each client's requirements.
- **Consultation and support**: Provide ongoing support and consultation to ensure optimal use.
- **API Integration**: Offer the services via APIs for easy integration.

***Key Resources:***

- **FRT**: Access to advanced FRT systems.
- **DLT**: Access to DLT
- **Customization expertise**: In-house expertise for developing customized solutions.
- **Customer relationships**: Establish strong connections with private sector clients.

***Customer Relationships:***

- **Consultation**: Maintain an ongoing consultancy relationship with customer to understand their unique evolving needs.
- **Training and support**: Offer training sessions, user support, and troubleshooting to ensure the smooth operation of IMPULSE

***Channels:***

- **Industry conferences**: Attend and participate in industry conferences to network and showcase expertise.
- **Online platforms**: Utilize digital channels, such as a professional website, to provide information and engage with potential clients.
- **Trade fair**: Promote the service through marketing campaigns and sales channels.

***Customer Segments:***

- **Private sector enterprises with unique needs**: Focus on businesses across various industries with specific identity verification requirements.

***Cost Structure:***

- **Development costs**: Cover expenses related to developing customized solutions.
- **Customer support**: Allocate resources for ongoing support and consultation.

***Revenue Streams:***

- **Customization fees**: Charge businesses for personalized solution development.
- **Maintenance and support fees**: Recurring fees for ongoing support.
- **Integration fees**: Billing for assistance with platform integration.
- **Subscription fees**: Charge private sector clients based on usage and features.

# Annex D Business Model Canvas description for Model 4

**Model 4: Subscription based Credential Management Business model (private sector, long-term)**

***Value Propositions***:

- **Scalable micro-credentials**: IMPULSE offers businesses a scalable solution to issue, manage, and verify micro-credentials for their employees, clients, or members.
- **Enhanced security**: Providing a secure method for storing and accessing micro-credentials ensures heightened security in private sectors.
- **Customization**: IMPULSE allows businesses to customize the micro-credentials based on their specific needs.
- **Cost efficiency**: Offer an affordable, predictable cost structure through subscription pricing, reducing the need for substantial capital expenditures.

***Key Partners****:*

- **Technology providers**: Collaborate with technology providers for software, security, and cloud infrastructure.
- **Regulatory agencies**: Collaborate with regulatory authorities to ensure compliance with data privacy and security regulations.
- **Consultants and experts**: Partner with industry experts to provide additional consultation or support services as needed
- **Private sector companies, professional associations, educational institutions, and industry groups:** Partner with those interested in adopting micro-credential solutions.

***Key Activities****:*

- **Platform development and maintenance**: Develop a platform for businesses to issue micro-credentials to their stakeholders and regularly update the platform with new features, enhancements, and security patches
- **Technical support**: Provide ongoing technical support to business clients.
- **Security monitoring and compliance**: Continuously monitor and enhance security measures and compliance with data protection regulations

***Key Resources****:*

- **Cloud Infrastructure**: Secure and scalable cloud infrastructure to host the eID and micro-credential management platform.
- **Software development team**: Employ a skilled team of software developers, security experts, and support staff to maintain and enhance the platform
- **Regulatory expertise**: Ensure compliance with industry-specific regulations and data security and privacy regulations .

***Customer Relationships****:*

- **Onboarding**: Assist organizations in migrating to the platform, configuring settings, and setting up their eID and micro-credential systems.
- **Training and support**: Offer training sessions and provide ongoing support for a seamless user experience
- **Feedback loop**: Establish channels for feedback, feature requests, and issue reporting to continuously improve the platform.

***Channels**:*

- **Direct sales**: Reach out directly to potential business clients and offer them tailored solutions.
- **Online marketing**: Promote IMPULSE through professional websites for online marketing.
- **Industry partnerships**: Form partnerships with technology providers, consultants, and industry associations for mutual promotion.
- **Industry conferences**: Attend and participate in industry conferences to network and showcase expertise.

***Customer Segments**:*

- **Private companies**: Target businesses across various industries interested in adopting micro-credential solutions.
- **Professional associations and Educational institutions**: Approach organizations that can benefit from offering micro-credentials to their members or students.

***Cost Structure**:*

- **Cloud infrastructure costs**: Cover expenses associated with cloud hosting, data storage, and network resources
- **Platform development**: Costs related to developing and maintaining the micro-credential platform.
- **Customer support**: Budget for customer support staff and resources.
- **Marketing and sales**: Expenses associated with marketing and sales efforts.

***Revenue Stream**:*

- **Subscription fees**: Generate recurring revenue through subscription fees, billed monthly or annually, based on the number of users or services.
- **Customization services**: Charge fees for customizing micro-credential solutions to meet the unique requirements of different clients.
- **Training and Support Fees**: Offer training and support packages with associated fees