Leveraging eIDin the Private Sector

D7.1 Report on Market Research and Feasibility Analysis

Document Identification			
Status	Final	**Due Date**	30/04/2018
Version	1.0	**Submission Date**	16/05/2018

Related WP	WP7	**Document Reference**	D7.1
Related Deliverable(s)	D7.2, D7.3	**Dissemination Level (*)**	CO
Lead Participant	ATOS	**Lead Author**	Aljosa Pasic
Contributors	AEGEAN , UMU, HMAR, ELTA	**Reviewers**	Petros Stefaneas, NTUA
			Adrian Fernandez Vega, Correos

Keywords:
Identity, eIDAS, market, feasibility, sustainability

This document is issued within the frame and for the purpose of the *LEPS*project. This project has received funding from the European Union's Innovation and Networks Executive Agency – Connecting Europe Facility (CEF) under Grant Agreement No.INEA/CEF/ICT/A2016/1271348; Action No 2016-EU-IA-0059 The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document Information

List of Contributors	
Name	Partner
Aljosa Pasic, Jose Crespo	ATOS
Thomas Macheras	ELTA
Elena Torroglosa	UMU
Antonios Stasis, Loukia Demiri	HMAR
Petros Kavassalis	AEGEAN

Document History			
Version	Date	Change editors	Changes
0.1	30/11/2017	ATOS	Table of content
0.2	24/01/2018	ATOS	Draft with indication of expected contributions
0.3	09/03/2018	ATOS	Interim draft distributed to partners
0.4	27/03/2018	ELTA	ELTA contributions and editing
0.5	04/04/2018	UMU, ATOS	UMU contributions integrated, ATOS editing
0.51	12/04/2018	HMAR, ATOS	Introduction chapter and revision of ELTA input done by ATOS, Policy chapter contribution and minor revisions done by HMAR
0.52	18/04/2018	ATOS	Editing of UMU inputs, merge of sections 3.1.2 and 3.2.4
0.6	18/04/2018	AEGEAN	Adding sections 3.2.2 and 4.1
0.62	19/04/2018	ATOS	Integration of new inputs from ELTA, AEGEAN
0.7	20/04/2018	ATOS	Additions to section 4 and 5
0.8	23/04/2018	AEGEAN, UMU	Update of section 3.2.2 and 2.3.3
0.9	25/04/2018	ELTA, ATOS	References moved, revision of chapter 4.1
0.92	26/04/2018	ATOS, UMU	Minor modifications and additions
0.93	27/04/2018	ATOS, AEGEAN	Executive summary update
0.94	08/05/2018	CORREOS,NTUA	Peer review
1.0	16/05/2018	ATOS	Final version after peer review and G.A
FINAL	16/05/2018	ATOS	Quality review and submission

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
API	Application Programming Interface
CIAM	Consumer Identity and Access Management
CIAM	Customer Identity and Access Management
Dx.y	Deliverable number y belonging to WP x
EC	European Commission
eIDAS	Electronic Identification and Signature
EUPL	European Union Public Licence
FIDO	Fast IDentity Online
GDPR	General data protection regulation
IAM	Identity and Access Management
IdM	Identity Management
IPV	Identity Proofing and Validation
LoA	Levels of Assurance
SAML	Security Assertion Markup Language
SLA	Service level agreement
SP	Service provider
SSO	Single Sign On
SWOT	Strengths, Weakness, Opportunities, Threats
TSL	Transport Layer Security
USSD	Unstructured Supplementary Service Data
WP	Work Package

Executive Summary

LEPS project enables existing services in the financial and postal sectors to use the pan-European elD infrastructure for cross-border electronic identification and authentication (i.e. eIDAS Network) and operate under elDAS specifications and rules. In this context, the project provides technical guidance to Service Providers in how to effectively integrate the (proxy) national nodes of the eIDAS Network, to relax "connection barriers" for Service Providers such as technical complexity, speed, and cost of integration. For such purpose, in this deliverable, a compacted market research and feasibility analysis of the uptake of the use of eIDAs services by the private sector (especially in the financial and postal industries) has been conducted, and operational and policy enablers have been identified. In this perspective, the document reviews previous related work, i,e. technical and business trends in this area, as well as essential conclusions from previous projects and initiatives, which are relevant for identity management and cross-border identification via eID-EU in the selected sectors and beyond. It also includes feedback in terms of feasibility and sustainability of the use of eID-EU, received by an Industry eID Monitoring Group thas has been established early in the project. The findings of this deliverable will be used in the project tasks that follow this initial analysis, namely in a detailed cost-benefit assessment of the integration with the eIDAS Network of a Service Provider and in the definition of a roadmap for maximizing the impact and the further use of LEPS outcomes. The essential contribution of this deliverable can be summarized as follows:

1. The cost and the operational effectiveness of the adoption of an eIDAS compliant eID service is one of the main concerns of the private Services Providers that should be addressed in priority. LEPS outcomes, essentially the concept of a stand-alone API Connector that can be easily deployed within SP's premises and interoperate with existing applications and operations modes, thus making integration with a (proxy-based) eIDAS Node a cost-effective and lean process, is a significant contribution in this regard.

2. The most interesting current trend in the sector, that appears also as the most influencing factor for the market uptake of eIDAS compliant eID services in the private sector, is mobile identification and authentication, which dramatically reduces costs while improving security and user experience. LEPS contributes in this regard via an Android OS App developed that ensures eIDAS compliant mobile authentication and attributes delivery required to get access to the e-services of Greek Service Providers.

3. One of the major barriers to the adoption of the eIDAS services is the relatively low level of cross-border transactions, especially in the financial and postal sectors. However, new regulation favoring increased competition, and ongoing globalization moves, are expected to reduce such barriers. In addition, the use of Customer Identity and Access Management (CIAM), an "imperfect" but widely adopted solution for "external" identification based in eID services provided by Social Networks and Internet mega-providers, raises in the current days significant security and privacy concerns, thus creating a "window of opportunity" for eIDAS compliant identification services. The development and promotion of best practices of eIDAS enabled authentication in cross-border operations might have a clear positive impact on the uptake of the use of eIDAS Network services.

4. A SWOT analysis conducted with reference to the adoption of eIDAS Network services shows strengths and opportunities (such as, for example, the rise of cross-border e-commerce in all EU countries and the thriving societal and political concerns about the use of fake digital identities) but also important weaknesses and threads mostly related to the low cross-border activity in several important sectors of the European economy, various inertia, and the still limited interest of e-service providers for high assurance eID services. Putting it in another way, the higher level of assurance provided by connectivity to eIDAS ecosystem is simply not enough for a wide market uptake. It is clear however that concrete value propositions such as provided by LEPS (based on the reduction of technical and cost barriers for Service Providers to integrate with the eIDAS Network) increase the feasibility of the operation.

5. Finally, the sustainability of the adoption of eIDAS eID services by private Servive Providers seems to depend on the extended and continuous partnership and collaboration between the providers of (the mosty) public infrastructures for identity data storage and provision ("notified" eiD providers, eIDAS Network nodes, and services etc.), and the private Service Providers using this infrastructure to enable eID bases authentication, It relates also to the existence of different scenarios for the evolution of the eID ecosystem, mostly defined on the basis of the specific operational characteristics of the "notified" eID providers (for example, regional clustering) and on the possible emergence of new players, acting as internmediaries in the value chain o of identification-authentication, like "eID brokers", Remote Proofing and Verification Providers (IPVs) and others.

1 Introduction

1.1 Purpose of the document

Activity 7 of LEPS project is dealing with technical, business and policy issues to maximize the adoption of cross-border identification and authentication services by the private sector. The main focus is on the domains covered by the pilot (Postal and Financial Sectors) with a minor effort spent on the analysis of other economic sectors in the context of online service provision that would start to use eIDAS eID building block. Within the activity 7, this deliverable is produced in task "Market Research and Feasibility Analysis of eIDAS services uptake by private sector". The main purpose of the document is to identify and analyse all sources of information necessary for conducting the work of the activity (i.e. outcomes from previous projects and initatives, relevant for eIDAS and for management of eID in selected sectors). Industry eID Monitoring Group was established early in the project and it was consulted in relation to the feasibility analysis. The conclusions of this deliverable will used for the next tasks in activity 7, namely cost-benefit assessment and roadmap and recommendations reports to maximize take up of LEPS outcomes.

1.2 Relation to other project work

This deliverable is taking input directly from all other work packages, especially in the chapter 2, which is dedicated to the presentation of project results.

1.3 Structure of the document

This document is structured in 5 major chapters:

Chapter 2 presents overview of projects results, with the clearly assigned intellectual property ownership and licensing. The initial assumptions related to the packaging and uptake are also presented. **Chapter 3** is the main part of the document and is dealing with market research and policy analysis from different perspectives, roughly categorised as demand and supply side perspectives. The major part is dedicated to demand side situation and perspective, having in mind that e-ID market is multi-sided and while online service providers are considered as the main customer target, the other stakeholders (e.g. eIDAS node operators, citizens) are also forming part of the demand side. In **Chapter 4** we are presenting initial feasibility and sustainability analysis, which will be complemented later with cost benefit analysis. The main issue here is likely technical and market feasibility, since the other elements (organisational sustainability, legal sustainability) are not depending so much on LEPS project, but on the status of eIDAS infrastructure after 2018 and support given by eIDAS node operators (e.g. service level agreements). Finally, **Chapter 5** is presenting conclusions that will be taken also to the next phase of the project.

2 Project Results Overview

2.1 Project Context and terminology

eIDAS (electronic IDentification, Authentication and trust Services) is used to denominate a variety of items or concepts in LEPS project. The original meaning refers to EU regulation on electronic identification and trust services for electronic transactions in the internal market, established in EU regulation № 910/2014. However, it also refers to a set of standards for electronic identification and trust services, parts of CEF eID Digital Service Infrastructure (for example when we talk about eIDAS "nodes"), as well as services (all electronic identification, authentication and signatures, as well as related ancillary trust services that are regulated under eIDAS regulation). Unless specified otherwise, eIDAS in this document will refer to cross-border electronic identification and authentication services that use eIDAS infrastructure and comply with eIDAS specifications and regulations.

The LEPS project focus is on integrating certified e-Delivery and e-Notifications (Correos Group), e-Delivery (ELTA) and remote e-signature services (Athens Exchange Group) with the eIDAS. From the perspective of project exploitation and market research, the main result could be technical service, namely "eIDAS specific system integration". However, more attention will be given to reusable software components, such as supporting tools, libraries or application programing interfaces (i.e. a mobile interface for authentication-attributes delivery, eIDAS interconnection gateways).

In addition, this deliverable focus is on the market potential of eIDAS in the private sector through the eIDAS node deployments, as well as faster and cheaper integration of services from private sector. Services that have been used for eIDAS integration in LEPS pilots are selected as representative for cross-border provision of e-services, as well as possible early adopters that would contribute to increase overall eIDAS uptake and use in private sector.

Finally, when it comes to intellectual property and licensing, we will consider existing components and open source licenses (e.g. CEF eIDAS-Node software, outcomes of STORK 2.0 and e-SENS projects, a connector component from UAegean),as well as new components (e.g. mobile authentication app from Universidad de Murcia (UMU).

2.2 Project Results Identification

Table 1: Project results identification

Name of result	Description	Reusability, IP and licence
Mobile App	An app (Android OS) developed to ensure mobile authentication and	Reusable, UMU (100%), Apache

Name of result	Description	Reusability, IP and licence
	attributes delivery required to provide a Spanish mobile ID for authentication to Greek services, based on the paneuropeaneID infrastructure complying with eIDAS specifications. The app will be available for download free of charge.	2.0
eIDAS adapter for Spanish node	The eIDAS adapter is a software component that offers an interface to service provider as REST endpoint. It can be deployed as a Docker container to improve portability and fast deployment and is currently provided as a service from Atos premises.	Reusable, provided as a service, ATOS (100%), EUPL 1.2
eIDAS SP SAML Tools Library	Java-based library for SP connection to eIDAS node (based on DEMO – SP))	Reusable, Aegean (100%), EUPL 1.2
eIDAS SP WebApp 2.0	eIDAS adapter developed as Web application that can be use by Java or non-Java-based service provider application.	Reusable, Aegean (100%), EUPL 1.2
eIDAS ISS 2.0	Interconnection Support service that can be used for Java or non-Java-based SP application interface (developed from scratch). It comes in two variants: with or without SP e-Forms / thin WebApp	Reusable, Aegean (100%), EUPL 1.2
System integration, service	The user interface and back-office adaptations	Partially reusable knowledge and code
Consulting, training or support services	Exploitation of acquired know-how	Partially reusable knowledge

2.3 Results Description Summary

In the previous chapter we listed a number of project results that help private service providers (SP) to make faster and cheaper integration of their services to eIDAS. In the subsequent analysis we will not enter into assessment of benefits of eIDAS, which is already well known with an important number of legal and security-related mechanisms and guarantees. The focus of LEPS project and this deliverable is on lowering down barriers for service providers, such as speed and cost of integration. However,

even providing “out of the box” eIDAS interconnectivity is not a guarantee of market success, given that the nature of eID markets is “multi-sided” and has to consider many other value factors.

We envisage several constraints for the wide adoption of eIDAS compliant cross-border eID services by online services providers. The first is that most of them already offer their customers the possibility to have personalized user accounts and “local” credentials, or to login to their sites and services through the credentials users already have from another online service providers, such as social networks. For this reason, the segmentation of our target audience has to take into account specific context of e-service provider, such as:

- Organisations that need or want to make migration from the existing identity and access management (IAM) solution. This could apply to organisations that have scaled out their internal or tailor made IAM solutions, or organisations that already use external or third party e-identification or authentication services, but are looking for the replacement.
- Organisations that want to open new delivery through mobile phone and are interested in mobile ID solutions that work across borders
- Organisations that use low assurance e-ID, such as social login, and want to elevate overall level of security and decrease identity theft and fraud by integration of external e-ID services with the higher level of assurance.

Therefore, the main targets of this study are service providers that are planning migration or extension of their current e-ID services, in the cross-border context.

eIDAS regulatory framework for electronic identification and trusted service provision brings an important value proposition to private service providers, which is legal certainty and liability, but the cost of integration and operational conditions are not clear for private sector e-service providers.

In technical terms, eIDAS e-ID ecosystem includes a network of national proxy nodes and so called “notified” IdPs providing different sets of personal and legal identity attributes obtained from authoritative resources. The combination of legal certainty and high assurance in the most cases of member states “notified” e-IDs, is elevating level of trust by both consumers, as well as service providers. However, the question that most private service providers raise is: how much will this adoption of eIDAS compliant e-ID services cost?

LEPS aims at answering this question and the project results presented in this chapter are offering several alternatives to service providers. Rather than cost reduction, we think that term “cost optimisation” might be more appropriate, since some service providers might opt for more expensive architectural solution in order to attain more control over eIDAS interconnection component maintenance or operations.

“The evolution of business models” and a “change in the mind-set” was mention in ENISA study on eIDAS adoption [1], as key factor for a wider uptake, while “ease of use, mobility and user experience” and “accessibility of free/open source libraries and open specifications” were also mentioned. All of these are present and analysed in LEPS value proposition, which will be explained in more details. eIDAS Network integration solutions and alternatives, ranging from “tailor made” to “off the shelf”, IAM solutions operated internally or consumed “as a service” should exist and compete. The main innovation in LEPS is the concept of a stand-alone API Connector that can be

easily deployed within SP's premises and interoperate with existing applications and operations modes, thus making integration with a (proxy-based) eIDAS Node cost-effective and lean process.

2.3.1 Value proposition

Successful connection of a Service Provider to the eIDAS Network is a multi-step process, already explained in deliverable D4.2. These five high level requirements can be summarized in the following list:

1. Familiarization with SAML communication (protocol understanding and implementation).

2. Implementation of the required web interface (UI) for User interaction with the eIDAS-enabled services.

3. Formulation and proper preparation of an eIDAS SAML Authentication Request.

4. Processing of an eIDAS Node SAML Authentication Response and provision of the appropriate authentication process end events for success or failure.

5. Publishing of the SP's metadata, as is required by the CEF eIDAS Specifications.

The main proposition from LEPS in this regard is saving cost and time for e-service provider organisations in regard to development and integration with eIDAS services. This can be done by reuse of the existing LEPS components. The intention is to made integration of eIDAS e-ID services as easy as it is today case with the social login APIs.

In the next deliverable D7.2 the cost-benefit analysis will be done with more details. This will be done having in mind different strategies and options for development and integration effort that service provider needs to make. The first option is tailor made or "from scratch" eIDAS Specifications Implementation. Service provider can also make custom solution based on "Demo SP" package of eIDAS Specifications Implementation. Finally, in this deliverable D7.2 we will look at cost of development and integration through reuse of LEPS components.

eIDAS Nodes main characteristics are describes in many EU project reports and studies. In Study on Cross-border Use of eID and Authentication Services to support student mobility and access to student services in Europe [26], for example, it was mentioned that they do not store any personal data and, furthermore, best available, state of the art technical solutions are used to protect privacy and confidentiality of exchanged data. In practice, SAML messages exchanged are signed by the sending parties (and verified by receiving parties). Signed SAML assertions within SAML response messages must be encrypted (SAML XML Encryption with AES algorithm is used). Furthermore, communication between eIDAS nodes is performed via the citizen's browser and to secure the transport layer of this communication between these components and the citizen's browser, Transport Layer Security (TLS) is used. All communication endpoints are securely identified. Use of a common syntax and standardised SAML message format between eIDAS nodes (used more than once between Member States and proven in operational environment) is allowing the proper processing of the minimum set of person identification data uniquely representing a natural (or legal) person, therefore introducing flexibility if service provider needs additional attributes relating to identification, which was the case for example of Correos and ELTA pilots. The second value proposition, in this respect, is related to the privacy, since the flexible architecture enables significant improvement in user-centric management of attributes.

2.3.2 Possible concerns

During the establishing of industry monitoring group of LEPS some issues were raise by it members. One of these issues referred to the service level agreement (SLA) offered by eIDAS node operators. In principle private service provider can expect a high level of availability / uptime of the national interoperability infrastructural components of the eIDAS Network, given the backing of the Member States and the liability aspects regulated. However, at the time of writing this deliverable there is no specific SLA or estimations if this will have any cost for service providers.

Another concern is uptake from countries different from Spain and Greece. In so-called middleware countries, e.g. Austria and Germany, the integration effort lies at the middleware, not at the SP, so these countries are not considered as the main target for LEPS study. For other countries a number of contacts has already been made through projects such as TOOPS or eIDAS 2018. In a matter of fact the inter-project collaboration is not seen only as a dissemination activity, but rather as a sustainability actions, since raising awareness about LEPS results is contributing to results transfer and adaptation, as well as creation of "eIDAS connection community". In this direction the following collaboration took place already:

- Aegean and HMAR are both participating and sharing results with TOOP - The Only Once Principle project (http://www.toop.eu/). TOOP demo architecture implementation incorporates LEPS APIs (WebApp 2.0). Task: Identify users accessing the services of a TOOP Data Consumer via eID_EU
- Atos has collaboration with CEF eID-FIWARE project. Since Atos is co-founder of FIWARE Foundation it is supporting publication of connectivity to CEF e-ID building block as generic enabler. LEPS adaptor for Spanish DNIe will be part of know-how exchange with UPM, partner responsible for generic enabler.
- Opening a bank account with an EU digital identity is another CEF telecom eID project and OIX is member of LEPS industry monitoring group. LEPS has been invited to their project event in September.
- ESMO (eIDAS-enabled Student Mobility) is CEF Telecom project coordinated by Atos and LEPS will be partially used there.
- Partners from eIDAS 2018 for Municipalities project are in LEPS industry monitoring group and there was already one webinar attended.
- Studies+ and ID4U have also been contacted for awareness raising and collaboration purposes
- Outside of CEF Telecom projects, other e-ID initiatives are in continuous contact either through IMG or participation in events. This includes Future trust, ARIES and Credential projects, as well as industrial initiatives EEMA (LEPS will be presented at their Annual Conference in June 2018 in London), ECSO, TDL, OIX, Kantara and OASIS.

Initial cost estimation from other implementations and pilots, including Stork and Stork 2.0 projects, where Atos was a coordinator show a high variability due to estimation errors or because some partners had more overhead, caused by their internal organizational structure. In LEPS an early agreement on cost categories was reached and Aegean, as the partner responsible for D7.2 Cost and Benefit analysis, monitored cost reporting for customization and integration activities, in order to avoid disparity between reported figures. Based on the final outcomes, that will be reported in D7.2, we need to make conservative or risk-aware approach to planning of resources since most of integrators will not have know-how that was available to LEPS partners.

2.3.3 Mobile app

An Android OS App developed to ensure mobile authentication and attributes delivery required to provide a Spanish mobile ID for authentication to Greek services, based on the pan european eID infrastructure complying with eIDAS specifications. The Spanish authentication through eIDAS infrastructure can be made using user/pass, software certificates and the Spanish DNIe 3.0, which offers NFC access to interact with mobile devices. The app offers an eIDAS browser compatible with any service that requires the eIDAS authentication of a Spanish user, giving support with support for to all these authentication means; that the app can be used to access to all the services providers that make use of eIDAS infrastructure using a single application, which is a great advantage compared to the model implemented in Spain for the use of the DNIe 3.0 that requires the installation of different mobile applications for each service. . The app will be available for download free of charge.

2.3.4 eIDAS adapter for Spanish eIDAS node

This software component is responsible for the interaction between MyIdentity service of Correos and eIDAS adapter in both ways. MyIdentityservice, which is considered as a "gateway service" for all other postal e-services, triggers the user authentication process making an authentication request to the eIDAS adapter. The eIDAS adapter will provide to MyIdentity service the user data according to the protocol and format established in advance. Given that these parameters are configurable, we consider software component reusable in any scenario that involves Spanish eIDAS node connection.

2.3.5 eIDAS SP SAML Tools Library

Service providers that use Java application and decide to developed connector to eIDAS from scratch might make use of this library in order to reduce costs. Additional value propositions are that they eliminate need for multiple certificates for each of services within SP that connects to eIDAS node and there is no need for pre-built user interfaces. Service provider would avoid extra development time for creating and processing SAML messages. The eIDAS SP SAML Tools library is offered in the form of a Java library, based on the CEF provided SP implementation (so called demo SP, see [3] for the latest version instructions).The library provides methods that a Java-based SP implementation can call to create SAML Requests (format, encode, encrypt), parse SAML Responses (decrypt, decode, parse)and create the SP metadata xml, as required by the eIDAS Specs.

The SP developer can specify, on a per request basis:

- The list of attributes requested
- The Nationality of the SP
- The Nationality of the Citizen/User to be authenticated
- The requested Level of Assurance (LoA) for this Service

The Java libraries which facilitate integration and communication with the Greek eIDAS Node come in lib.zip file that was used in LEPS pilots.

2.3.6 eIDAS SP WebApp 2.0

This web application is available for both Java or non-Java-based service providers (SP). Advantages are similar to tools library, but in addition it reduces development time by completely handling an eIDAS-based authentication flow (including UIs). It is also infrastructure independent since it operates over a simple REST API. Finally, use of JSON web tokens (JWT) increases overall security level.

In order to use the WebApp 2.0 for integration with the eIDAS Greek node, it needs to be deployed in the same domain as the SP, which was perceived as a limitation in the pilot. On the positive side configuring the SAML library and the configuration of the eIDAS WebApp 2.0 is rather easy and flexible mechanism that enables reusability. This WebApp is offered as a Docker image which is in principle optimal solution, but in order to deploy the WebApp 2.0 the hosting machine must have a functional Docker engine. Therefore service provider needs to know how to setup Docker (or should use system integrator services). In LEPS pilot this component is tested with ELTA eDelivery hybrid service.

2.3.7 eIDAS ISS 2.0

Interconnection Supporting Service (ISS) comes with or without SP e-Forms, and in the latter case we refer to ISS thin WebApp. Benefits for service provider are similar to the previous cases in terms of saving development cost and time (e.g. reduction of development time for processing SAML messages), but in addition it supports the interconnection of many SP services in the same domain (each service is managed via a thin WebApp) to eIDAS node. It sends SAML 2.0 request to eIDAS Node and translates response from SAML 2.0 to JSON and other common enterprise standards(such as WSDL) and forwards it to the relevant SP service. Multiple services within the same SPs are sharing one certificate. Therefore it enables SPs to communicate with the eIDAS Node without using SAML 2.0. Each request can be parameterized (explained below) by:

a. the Attributes requested

b. the Citizen/User Nationality

c. the Level of Assurance Requested

Thin WebApp version complements ISS 2.0 functionality by containing a pre-built UI. The retrieved attributes get bundled together as a JWT token that arrives to the SP in the form of a cookie (auth_token).In order to use the Thin WebApp for integration with the eIDAS GR node, a fully functional instance of the ISS 2.0 service must be deployed.

In LEPS this component is tested with integration of 3 services provided by ATHEX and 3 services provided by ELTA.

2.3.8 eIDAS service package: System integration, consulting and training services

This project result is not tangible, but for the company such as Atos it might present an opportunity since accumulated know-how can result in a number of business opportunities. Typical offering starts with consulting phase that identifies the specific requirements including an initial assessment to determine what level of identity assurance is needed, what channels will be used for service provision

etc. Assessment includes consulting on regulatory issues, such as general data protection regulation (GDPR), for example related to the minimum set of data: what data will service be using and storing, including additional attributes not contained in eID. Once consulting phase has completed an initial assessment we could help to determine architectural options and investment needed in integration with eIDAS, as well as back office customisation. To facilitate this process, we might use data from cost and benefit report (D7.2) facilitated by LEPS.

The system integration phase of "service package" includes technical assessment of the specific needs and design of message flows. Support is offered in interaction with eIDAS node Single Point of Contact. The main activity is dedicated to customisation and integration with eIDAS eID service and complete end-to-end testing. LEPS components that produce and consume SAML are reused to reduce cost. Migration and deployment in a live production environment can be complemented with communication plan for the launch and ongoing operation of online service (a kind of managed operation service for online service providers), as well as training for the operational staff.

3 Market Research and Policy Analysis

In this chapter we used external sources of information, necessary for conducting the work of the activity (i.e. outcomes from eSENS, STORK 2.0, SSEDIC, FutureID, EC and other European institutions consultations and studies like EBA Green and Discussion Papers, EC meetings with the industry, EBF Blueprint for Digital Banking, etc.). An Industry eID Monitoring Group was established in order to channel communication related to the market analysis, cost-benefit assessment and roadmap and recommendations reports to maximize take up of LEPS outcomes. Some of the sources used in this chapter are received from IMG members. eID issues and challenges related to wider adoption have been, for example, commented in [12] with the limitation of scope to Nordic countries. Sectorial associations, such as European Banking Authority also published discussion papers [13].

Many of the previous sources, however, are already outdated and new trends emerged in digital service arena, such as the shifting of users, applications and management to the cloud, and the acceleration of mobile identity. Derived credentials and privacy preserving technologies already existed in the time that Stork project was running, but their adoption was rather low. With the new general data protection regulation (GDPR) these technologies also started to play a significant role in several e-ID ecosystems. Finally there is a trend of separation of different e-ID services provided from the cloud, so that we can see, for example, identity verification and proofing being done by one provider, while the later usage (e.g. authentication) is managed by another.

From all these trends, the one that is most promising to impact market uptake of eIDAS compliant eID services by private service providers is mobile identification and authentication, which dramatically reduces costs while improving security and user experience. Given the fact that it is also one of the LEPS outcomes, we will dedicate one chapter to trends related to it. Other trends related to this irruption of mobile identity will be left out of scope. Local biometric authentication for mobile phones, for example, shows potential but will require time because the Fast IDentity Online (FIDO) standards are still evolving.

As mentioned previously our main focus is on e-service providers in postal and finance sector where many organisations made important investments in their internally operated IAM solutions. These solutions, however, are originally not meant to handle the requirements for large scale cross-border e-service use cases, although the functional building blocks and protocols are the same. This fact was exploited by social network and other online service provider to offer their “identity APIs” as an easy way to integrate highly scalable, yet low assurance, e-ID services. More recently, so called customer IAM (or CIAM) appeared as a segment separated from traditional IAM, with the focus mainly on vendors that offer some sort of “identity cloud” (other terms that are used include “Id-as-a-service”, Identity federation hub, identity gateway etc). In Figure 1 we present the main differences between traditional IAM solutions, that can be operated internally or externally, and the new generation of CIAM solutions. Some of these solutions integrate API gateways, for example CA technologies, or Okta, as well as support for mobile ID.

With scalability, there are other requirements that might depend on a specific e-service provider, such as for example integration with customer relationship management or handling a single customer with many identities. One of these identities, in the future, could also come from eIDAS eID ecosystem, in other words could be “notified e-ID” of the customer. Another solution could be to use the “notified e-

ID" only for the enrolment, in the phase of identity proofing and verification, while virtual or derived e-IDs are used for posterior e-ID services such as authentication. In the following chapters we will look at these possibilities.

Traditional IAM	Customer IAM
Manages **employee identity** within a corporation.	Manages **customer identity** on digital customer-facing multi-channel sites (web, mobile, IoT).
Users are **being signed up** by company, with key profile data being filled in by HR or IT.	Users **sign up themselves** and **generate user-specific data** on their own.
Authentication against internal **directory services.**	Authentication against public services like **OpenID** and **social media**, as well as **directory services.**
Users are **known** and captive: employees, contractors, partners. **Trust is assumed.**	Users are **unknown** (until registration) and may create multiple and fake accounts. **Trust cannot be assumed.**
Workforce users are typically **tolerant** to poor performance and latency and **can't easily change.**	Customers and prospects have **very low tolerance** for poor performance and **have many choices** of competitive alternatives.
Scalable to **10s to 100,000s** users, one identity each.	Scalable up to **100s of millions** of users with up to **billions** of consumer identities.
Many heterogeneous IT systems, on a **closed, corporate** network.	Many heterogeneous IT systems, on **public** networks (Internet).
Identity Provider (IdP) is typically **one central** internal IT system.	**Many decentralized** Identity Providers – Social Login through Facebook, Google, LinkedIn, etc., and traditional login.
Employee profile data collected for **administrative and operational purposes.**	Customer profile data collected for **highly critical business purposes** (transactions, marketing, personalization, analytics and business intelligence).
Integration with **HR and ERP** systems.	Integration with a broad landscape of **marketing and sales automation** technology, **analytics systems**, and **security and compliance** solutions.
Management of personal data and user privacy/preferences/ consent happens only within a tightly **controlled homogenous corporate environment.**	Handling of personal data subject to a **broad variety of privacy and data protection regulations** that differ between regions and require to enable users to view, modify and revoke preference and consent settings.

Figure 1: Comparison of traditional IAM to customer IAM solutions (source: Forrester)

3.1 Market description and trends

3.1.1 Notified e-ID ecosystem

In this chapter we look at the situation related to the adoption of notified e-ID across Europe. We should not forget that the uptake of these e-ID services has to parts: one is "within border" use, where both identity provider and e-service provider are belonging to the same member states, and another one is "cross-border" use of notified e-ID, rather modest so far, but expected to grow after eIDAS

regulation comes into force. “Within border” use has been existing for many years (one of the first e-ID cards was issued already 20 years ago) and the problem of adoption by the private service providers has been studied extensively. Some lessons were learned from the early experiments e.g. in Finland.

Today, all over the world national e-ID schemes, as well as mobile eID, increase in number, visibility and reach. It seems that the right opportunities exist both at the demand side (identity providers, service providers, citizens) and on supply side (technology providers).

eIDAS Regulation is providing already an excellent basis for identity ecosystem deployment, especially when private sector becomes aware of its advantages, but may lack impact when it comes to large number of e-service providers, that do not have high assurance requirements. In this document we also refer to eIDAS e-ID ecosystem as the cross-border use of notified e-ID, in line with definitions and procedures stipulated in eIDAS regulation. Notified e-ID solutions refer to eID issued by the government, on behalf of government or under the control of government. This ecosystem is still in its inception phase so the most of figures in this chapter will remit to the experienced from “within border” use of notified e-ID.

The overview of these EU member states solutions is given in figure below, which is reproducing situation reported to CEF website [2].

Country	Name of the eID scheme	Type	Status
Austria	National Citizen ID	Multimean	In use
Belgium	National ID	Smartcard	In use
Bulgaria	National ID	Smartcard	In development
Croatia	e-Citizen	Multimean	In use
Cyprus	ARIADNI	Login	In use
	National ID	TBC	In development
Czech Republic	National ID	Smartcard	In development
	mojeID	Login	In use
Denmark	NemID	Login	In use
Estonia	National ID	Multimean	In use
Finland	FINeID	Certificates	In use
	TUPAS	Mobile	In use
France	FranceConnect	Login	In development
Germany	National ID	Smartcard	In use
Greece	ERMIS portal	Login	In use
	National ID	Smartcard	In development
Hungary	eSzemelyi	Smartcard	In use
Ireland	MyGovID	Login	In use
Italy	SPID	Multimean	In use
	National ID	Smartcard	In development
Latvia	eParaksts	Smartcard	In use
Lithuania	National ID	Smartcard	In use
Luxembourg	National ID	Smartcard	In use
	LuxTrust	Multimean	In use
Malta	National eID	Smartcard	In use
Netherlands	DigID	Login	In use
	eHerkenning	Login	In use
	Federation: Idensys, iDIN, DigID	Multimean	In development
Poland	National ID	Smartcard	In development
Portugal	Cartão do Cidadão	Smartcard	In use
	Chave Móvel Digital	Mobile	In use
Romania	National ID	Smartcard	In development
Slovakia	National ID	Smartcard	In use
Slovenia	eUprava	Certificates	In use
Spain	National ID	Smartcard	In use
	Various*	Certificates	In use
	Cl@ve	Login	In use
Sweden	Bank ID	Multimean	In use
	e-Legitimation (Telia)	Multimean	In use
United Kingdom	GOV.UK VERIFY	Multimean	In use

Figure 2: Overview of eID schemes in Europe (as of March 2018, source: EC website)

At the time of writing this deliverable, however, only Germany officially notified its eId scheme, while Italy did pre-notification, with a federated scheme including public and private bodies. Other countries, such as Luxembourg have started pre-notification procedures. Thus changes are still expected to happen. As we can see in figure 1, in some members states e-ID card does not exist, so we might distinguish several cases of possible "notified eID":

- eID directly issued by the government, but not in a form of e-ID card;
- eID issued on behalf of the government, derived from government identity "root" eID or issued under the responsibility of the government (e.g. Swedish or Norwegian BankID);
- eID marketplace, with multiple providers, such as in Italy

For government issued eID, breeder document is considered to be birth certificate or similar. The pattern, or chain of identities is typically: national identity register (e.g. birth register), followed sometimes by state issued identity (not all countries have this), followed by one or more endorsed identities.

In LEPS project, Spanish and Greek issued e-IDs are used. These are not (yet) officially notified to the EC, but this is likely to happen during the execution of LEPS project. In Spain there are several e-ID schemes that are likely to be notified, including Cl@ve that has over 5 Million users and handles over 8 Million authentications per year in Spanish public sector. However, the focus here is on national e-ID card, that will be used in cross-border private e-service context.

Every Spanish citizen over 14 years old must have the Spanish National Identity Document (DNI). The first DNI as such was issued in Spain on March 20, 1951. The first model included data such as the profession or position and distinguished between four categories depending on the economic situation of the owner. In 1962, its design was updated and other data were included, such as blood group and marital status. It was not until 1981 when, with the constitutional shield, the economic categories were eliminated. In 1990, the national computerized identity document was introduced in Spain, in which the fingerprint disappeared and two lines of OCR characters were incorporated. It was in 2006 when the electronic ID began to be issued, a polycarbonate card engraved with laser and identical measures as a credit card that presented a chip with personal information and digital certificates for authentication and electronic signature.

In December 2015, the DNIe 3.0 was launched, which incorporates a Dual Interface chip that allows connection with telematic services both through a card reader and through the NFC technology available on many smartphones and tablets. The use of NFC aims to avoid the need for the installation and configuration of specific readers that were the main obstacle for the implementation of the previous version based on a traditional chip. The use of new DNIe 3.0 required the installation of additional software to allow the interaction with the Internet browsers and native applications on computers and laptops. In the case of smartphones (with NFC support) is required the installation of specific native mobile apps for each service that the user wants to use. The use of DNIe today is mainly on public sector services to pay taxes or do administrative transactions, and more recently its use is increasing in the private sector, specifically in access to banking services. Number of identity related transactions in public sector e-services is estimated to be over 25 Million in 2017 [14], while data for private sector is not available. More recently a vulnerability discovered by Czech researchers[1] has been also affecting Spanish national e-ID card. The effect of this event on national e-ID adoption is still to be evaluated.

[1] https://crocs.fi.muni.cz/public/papers/rsa_ccs17

One of the main value propositions related to notified e-ID ecosystem is that in the most cases it offers high level of assurance of e-ID. Stork deliverable D5.2.5 lists benefits for banks that include:

- Improved quality of the service offered to the customer;
- Improved Know Your Customer to reduce fraud and money laundering: The introduction of a process of identity check and recognition through eID reduces frauds.
- Reduction in operational, legal and reputational risk as trusted identities and authentication is provided by national public member state infrastructures;
- Time savings, reduction in terms of administrative overhead and costs;
- Increase in trust with the provision of a qualified digital signature that enable banks to trust that the information provided in the signed document is reliable ;
- Increasing potential customer base;

The eIDAS regulation mandates to establish three Levels of Assurance (in some government guides, like UK, called “assured identity levels”) , which categorize the notified eID schemes according to their security, covering the complete lifecycle of the credentials, including enrolment, issuance of the credentials, usage and finally revocation, as it was explained in [25]. The eIDAS Expert Group beyond this decision decided to go with an “outcome based approach”, i.e. not requiring concrete technology to fulfil security goals, but stating the fulfilment of a security goal itself as the requirement for LoA. In some member states it will be challenge to map levels into LoA and to match solutions from different MS into three levels, namely low, substantial and high.

The main driver for increased demand for higher LoA by service providers is related to the rise of identity fraud. Recent study shows that of the 3.1 million complaints received in 2016 by Consumer Sentinel Network [4], which is operated by the US Federal Trade Commission (FTC), 1.3 million were identity fraud related, costing consumers over $744 million. The median amount consumers paid in these cases was $450. According to another study issued by Forrester [5], 66% of respondents state that customers are demanding stronger online security and privacy protections. This study also lists several trends will have a dramatic impact on eID budget priorities, architectural decisions, the vendor landscape, and deployment options. In Ponemon institute study [6] two figures are especially interesting for LEPS analysis. The first one is on effectiveness of approaches to stop unauthorized access to information resources. While 74% agrees that a single factor authentication is no longer sufficient to effectively protect access to online services, only 50% believes that multi-factor authentication is the right answer and is effective at reducing risk posed by identity fraud. So what the other 24% respondents thinks? Probable answer is that at least one of the factors must have higher level of assurance.

3.1.2 Mobile ID solutions

The first demand, when it comes to technology adoption and acceptance of innovative and technologically superior security solutions, by common citizens, is usability and user-friendliness. Problems with smart card readers usability were ubiquitous also in every and each one of smart card based eID implementations in EU member states, regardless of their cost or security properties. In Germany card readers were distributed free of charge during the start-up phase to speed up the use of online identification, but this was still not sufficient to raise market uptake. The end user support was

another obstacle for the uptake since the variety of products and software should be compliant with the use of a specific smart cards.

With the advent of smart mobile phones, however, the whole new set of possibilities was opened in terms of balancing security and usability.

Apart from the traditional mechanisms for user authentication based on username and password, the increase in technologies and capabilities of mobile devices opens a wide range of options to create and improve the process of user authentication and security improvement. The new cryptographic capabilities integrated in mobile SIMs, the large increase in computing capacity and the new interfaces (such as the NFC) of smartphones are some of the available examples.

A number of options for mobile authentication exists, such as HTTP Header silent authentication, USSD (Unstructured Supplementary Service Data, sometimes referred to as "Quick Codes" or "Feature codes"), PIN, SMS+URL, SMS OTP (short message service and one time password), different types of biometric (fingerprint, face recognition), use of FIDO U2F, Mobile PKI (SIM based), as well as the already mentioned or traditional methods including username and password or social login.

Majority of today's mobile ID ecosystems are usually similar to centralized Public Key Infrastructure-based scheme and differ in the way the identity data is stored and managed, such as:

- SIM-based mobile ID: Data is physically stored on the SIM card of the mobile device. In some countries e-ID card is used as SIM card (Estonia, Moldavia).
- Embedded mobile ID: Relevant identification data is stored in the embedded secure element (SE) of the mobile phone. Most governments still have concerns about data privacy when it comes to storage of government issued eID not entirely under their control. Storing the government issued electronic identity in a USIM, microSD or SE, therefore appears to be unacceptable to most governments.
- NFC-based mobile ID: This solution uses the contactless NFC interface of the mobile device to securely access identity and authentication information from an external e-ID card. This is the case of Spanish DNIe 3.0 card which is also used for LEPS pilots. Key requirements for contactless smart card readers reading contactless government eID cards are the greater field strength required from the reader to power the card, and that the reader might need to support extended length APDUs to transfer longer pieces of data. At the moment the field strength issue seems to be less of a problem for NFC mobile devices then the "extended length" problem because extended length APDUs are not supported by the majority of smart phones today, although this is changing.
- Server-based mobile ID: In this approach, secured identity and authentication information is stored on an external server, which can be accessed using a mobile phone. This solution is implemented in Austrian government m-identity scheme.
- Derived mobile ID: A derived mobile ID is a special form of mobile ID set up from deriving credentials from government issued e-ID. A derived electronic identity could be limited to a digital certificate, enabling identification, authentication and electronic signature services, while satisfying government concerns about protection of citizens data. Australia Post's Digital iD service is an example of this type of e-ID. It verifies an online user's identity using documents such as driver's licence and passport, smartphone apps and QR codes.

Good overview of government driven initiatives regarding the mobile ID is given in [27]. In Austria and Estonia, mobile ID solutions are on the rise, but in the rest of EU only a small number of European member states have implemented mobile IDs so far. The Austrian („Handy-Signatur“) as well as the Estonian mobile eID (“Mobiil-ID“) can already be used for online authentication for electronic services (e.g., e-government, e-banking). Austrian model does not require any additional hardware and can be used on any mobile phone. The eID data are stored in the mobile ID system’s database in cloud, not on the mobile phone. There are more than 500,000 active mobile ID users with 10,000-15,000 uses per day and in a matter of fact mobile ID activation was 15 times higher than traditional eID card activation.

Estonia mobile ID relies on the SIM-based approach because at the time it was launched there was a lack of NFC devices in the market to reach a significant percentage of the population. The SIM card uses the same PKI as the eID card and the credential data is stored on a secured SIM card in the mobile handset. Citizens in Estonia access broad range of from their Mobile. 99.6% of banking transactions in Estonia are now done electronically and the country was the first in the world to allow m-Voting in the national Parliamentary elections with 3% of all votes conducted via mobile phone with help of Mobile-ID (Mobiil-ID), already launched in 2007 as an extension of the digital ID scheme. Mobile-ID can be used with over 300 organisations in both the private and public sector, according to e-Estonia.com, with around 40,000 users.

Similar to Spanish DNIe 3.0 that was used in LEPS pilot, use of German contactless eID card with NFC mobile phones is currently an ongoing effort. The German Federal Office for Information Security and the Bundesdruckerei has identified several smartphones and versions of Android middleware and applications that enable the German eID card to be used to provide mobile identification and authentication services to German citizens. The Open eCard open source initiative has developed an Android app that uses the German eID card for cloud authentication. Ageto, a company developing eGovernment software that supports the German eID card, also released an Android middleware. However, German situation is different from Spanish, given the fact that national e-ID relies on middleware that is installed at service provider site.

In LEPS pilot mobile app is based on the third version of the DNIe, that has a dual interface chip and allows NFC access (it is ISO 1443-compliant) to the electronic information of the smartcard. As mentioned before, ecosystem around DNIe is mainly composed of public service providers, with only few private service providers accepting this proof of identity, so the expectation is that enabling easy integration for m-service providers would extend this ecosystem and speed up the adoption.

On the public sector side, there are available different mobile apps to be download, provided by Spanish National Police and FMNT (“Fábrica Nacional de Moneda y Timbre”), that give access to a wide offer of public and administrative services such as social security and traffic procedures, tax payments or digital signature (e. g. “Portafirmas” app from University of Murcia). On the private sector, there are some initiatives that are focus, as us, to take the DNIe one step further. This is the case of Telefonica and Secuware, which are working on moving the DNIe to the mobile SIM card. The project, called mDNI , makes use of a PC to read the internal DNIe information and save it inside the user mobile SIM, which has to offer cryptographic capabilities to protect user certificates and keys. All these examples show direct relationships between the service providers and the identity providers, simpler flows than the eIDAS flow that always involves the interaction of the intermediate nodes of the Member States involved.

Among international non-governmental mobile ID solutions, probably the most interesting one is Mobile Connect, supported by GSMA. The Global System for Mobile Communications Association

(GSMA) is an international association that brings together more than 800 mobile phone operators around the world. The GSMA Identity programme is one of the GSMA's top priority programmes, which has developed Mobile Connect, a digital identity solution that offers a safe, seamless and convenient consumer experience, a consistent user interface and low barriers to entry across the digital identity ecosystem based on use the mobile number (named the telephone number) as user unique identifier.

The service works with any type of terminal and makes use of the encrypted system linked to the SIM card of each phone, then depending on the company and the SIM capabilities (PKI or no-PKI), Mobile Connect can ask the user to validate her identity by entering a code number, the fingerprint or with the acceptance of a message. GSMA calls these: authenticators. An authenticator is a technology that offers the means for the end user to establish her identity.

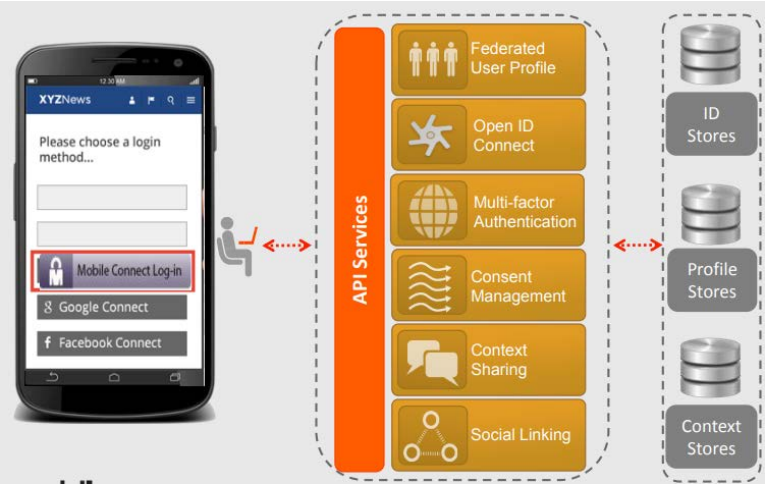

Figure 3: Mobile Connect and API exchange (source: APIGee presentation)

GSMA defines three options to authenticate the user: validate the process through an SMS to the user mobile phone, install an app in the user's mobile phone and combine it with SMS reception, and install an advanced app that makes use of advanced SIM capabilities such as PKI functions (only new SIMs have support for these features, it can requires SIM upgrades by the user/operator). The election of which authenticators will be offer to the user for the operator implies different cost of implementation and use usually assumed by the Operator

Depending on the selected authenticator, the method will have a Level of Assurance (LoA) between 1-4. Authenticators that only verify that a person pressed "OK" on the mobile phone have a low level, whereas a multi-factor authenticator will have a higher number. An online service provider may request a certain LoA to authenticate the end user.

It is important to note that at this moment the Mobile Connect LoA only describes the quality of the authentication method, not the identity information. The quality of the identity is related to the registration process and how the user identity has been verified when he acquires her mobile phone subscription. In most markets, to obtain a mobile phone the user need to verify her identity.

It is important to stress that Mobile Connect is currently running pilot, also co-funded by CEF, related to eIDAS integration. In addition, many of CIAM providers covered in the next chapter, already offer support for Mobile Connect in their identity gateways. The first pilot in 2015 was launched to enable Mobile Connect compliance with eIDAS. Mobile Connect uses the standard Level of Assurance (LoA) definitions from ISO 29115 for authentication: a global standards-based approach to authentication

security. LoA3 is a high-security two-factor authentication solution. LoA4 requires, in addition to LoA3, that the security credentials are based on PKI technology. In practice, LoA3 is comparable to European eIDAS directive defined security level “substantial” and LoA4 is comparable to “high”.

The pilot from 2017 involved 3 national eID systems authorities and eIDAS Node single point of contact from France, Norway, and Sweden. France Connect, where French postal operator La Poste acts as one of identity providers, was providing access to their eIDAS Proxy Node in its test environment. Launched in June 2016 by the French Government, France Connect is likely candidate to become “notified eID” system. From November 2017, “Mobile Connect et moi” has been launched and available to every citizen on France Connect portal along with other identity providers. Two members of LEPS industrial monitoring group (GSMA and Ariadnext) were involved in this pilot and the objective for Mobile Connect is now to enable other operators to join the initiative and launch the solution in other European countries

3.1.3 Identity APIs and CIAM

Online service providers that need to identify and authentication their web site or mobile app users have several options for this. One is to deploy and operate their own identity management system, either licensed off the shelf solution or tailor made e.g. based on some of the open source IAM solutions. Another one, much more frequent when it comes to e-services for consumers, is the use of external e-ID services and integration of these through so called “identity APIs”.

While so called “API economy” has been around for a while, it looks like the paradigm is now mature for wide adoption, according to some market analyst [7]. According to Forbes, “organizations and their IT teams are starting to focus more on unique API consumption strategies first”.

In a matter of fact, many businesses have first tried to scale internal solutions for external identity management purposes, but capturing, protecting and leveraging highly scalable customer identity data requires huge investment, so that later they migrated or decided to integrate option for external e-ID services. Reuse of the existing e-ID, such as social network login, is by far the most convenient option, preferred by the most e-service providers.

The focus is mainly on consumption of real-time e-ID services such as authentication. The Google OpenID API lets third-party web sites and applications let visitors sign in using their Google user accounts that uses OpenID standard. Google also offers other APIs such as web authentication of Google client authentication, for web-based applications, that allows the application to access a Google service protected by a user's Google account. The Facebook connect API enables login using the Facebook account, as well as the ability to request and display some additional Facebook account information. The Keystone Identity Service is API that allows clients to obtain tokens that can be used to access OpenStack cloud services. The Identity Link API returns data associated with reputation management, fraud reduction, and machine learning management. In principle Touch ID from Apple could also be included in this category of social login solutions. These are only few example of identity APIs that reduce time and cost for application or online service developers.

Implementing social login might be good for bridging the gap between usability and security, but it fails when it comes to high level of identity assurance, even the main players, such Facebook and Google improved their security features with multi-factor authentication, remote logout and unauthorized activity detection. The main problem with these solutions remains the first step: self-enrollment without any strong identity proof, such as government issued e-ID. Assurance is not the

only problem with the use of social network login for cross-border e-services. Citizens are increasingly aware of the privacy issue and 71% of consumers state that they are very concerned about online companies selling or sharing information about them without their permission (Consumer Reports), while 11% of adults admit to having abandoned an online purchase because the site asked for too much information (Forrester). There are also concerns about what private information they're giving up when they use social login. When it comes to use of social login by mobile apps, Facebook authorization, for example, can ask for up to 40 different permissions, ranging from access to photos to list of friends and more. It is up to the mobile app developer to decide which ones are required for a particular app, and which ones are optional, but expect one or two they all require review by Facebook before the app is published. Google + and Twitter enabled apps ask for much less permissions, on average, while Linkeid is generally considered as the most privacy respecting social login. On a positive side, integration of social network logins (e.g. through Connect API from Facebook) is fairly straightforward. It can take from several hours, in the that website is built with some framework that has built-in authentication modules (e.g. Django), up to few months if there is pre-existing tailor made authentication software that needs migration and other services.

More recently identity verification APIs appeared on the market and their adoption is very fast, especially on mobile devices. One example is Socure's ID+ solution that includes a series of modular offerings via a single API to validate consumer's identity data through correlation of the identity across 300+ certified offline, online and social data sources as well as provide predictions on the authenticity (whether the identity is real or not) and fraud risk of the individual. A different approach is taken in AriadNEXT's facial recognition API service, which is comparing selfie taken by mobile phone with picture from eID card. Trulioo's electronic identity verification (eIDV) platform, Global Gateway, and related API is another example aiming to automate ID checks and reduce integration time.

Besides direct integration of external e-ID services through the identity provider available APIs, e-service providers have also an option to use broker or aggregator of different identity providers that might offer additional functionalities, such as proxy to mobile devices, protection of consumer privacy and processing some data. One example is Gigya which has been recently bought by SAP. Other competitors include LoginRadius, Microsoft Azure AD, Janrain, Ping, Social Annex, Addshoppers, Ubisecure, Okta or OneAll. These solutions are sometimes called Identity clouds or CIAM (customer identity and access management) solutions. CIAM claims many measurable benefits and return on investment, such as 20-30% more efficient marketing & sales, reduction of the abandonment rate during the registration (that can be as high as 70%), or savings through simplified and unified infrastructure. The business model of CIAM vendors is based on charge per user or per transaction and implementation usually takes from 4 to 6 weeks. For e-service provider there is no large investment since identity is provided from the cloud and support is given by CIAM operators. Many CIAM vendors see eIDAS also as an opportunity. One vendor, for example, is already offering gateway to a kind of federation network (although national), namely Finnish Trust Network (FTN), which is a cloud-based mechanism for connecting large scale, consumer facing services with trusted identity and service providers. The Finnish Trust Network not only relies on eIDs issued by the government but also recognizes the electronic identities issued by commercial identity providers such as banks and mobile operators. In [12] also mentions Swedish federation of IdP and that "direct federation between the Nordic IdPs would in theory be possible", having in mind that Danemark, Norway and Iceland have one single IdP for e-government services.

In Germany SkIDentity Service (skidentity.com) is a kind of broker (see Figure 4: German Skidenity service) for service providers that can use popular social logins such as LinkedIn and Facebook Login,

as well as eIDAS eID services from a number of countries. eIDAS brokerage was activated in 2017 and now enables strong authentication and identification with support for various international identification documents in cross-border processes. In Netherlands, similar broker role to municipal e-services is provided by Connectis with support from CEF project (https://eidas2018.eu). The 81 participating municipalities opened up 200 public services to European citizens and representatives of Dutch businesses in the possession of an eID. The Connectis Identity Broker also works with non eIDAS identity providers and has Java and ASP.NET adapters to allow developers to easily connect their application. This broker is similar to LEPS ISS and is delivered as a java library (jar) or .NET library (dll) and integration with a typical application can be done in 10 to 25 lines of code. In Figure 5 it is depicted what is the current offering, both on IdP , as well as service provider side. The other brokers envisaged in the project, which is under the lead of Dutch Ministry of economic affairs, include Digidenity[2] and KPN[3].

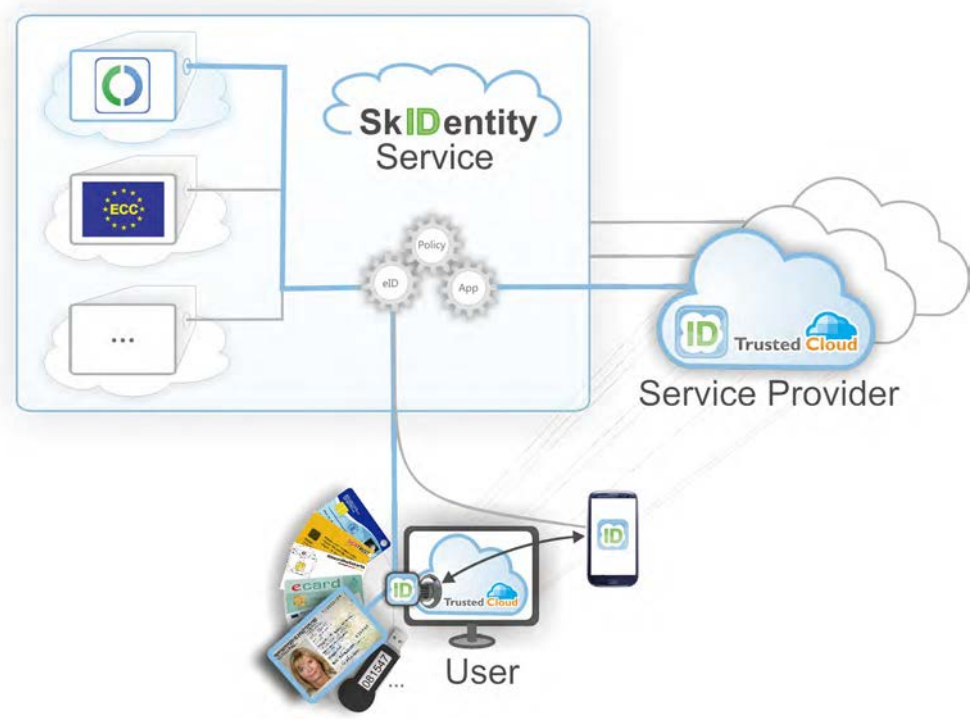

Figure 4: German Skidenity service

[2] https://www.digidentity.eu/en/home/
[3] https://eherkenning.kpn.com/dienstverleners/

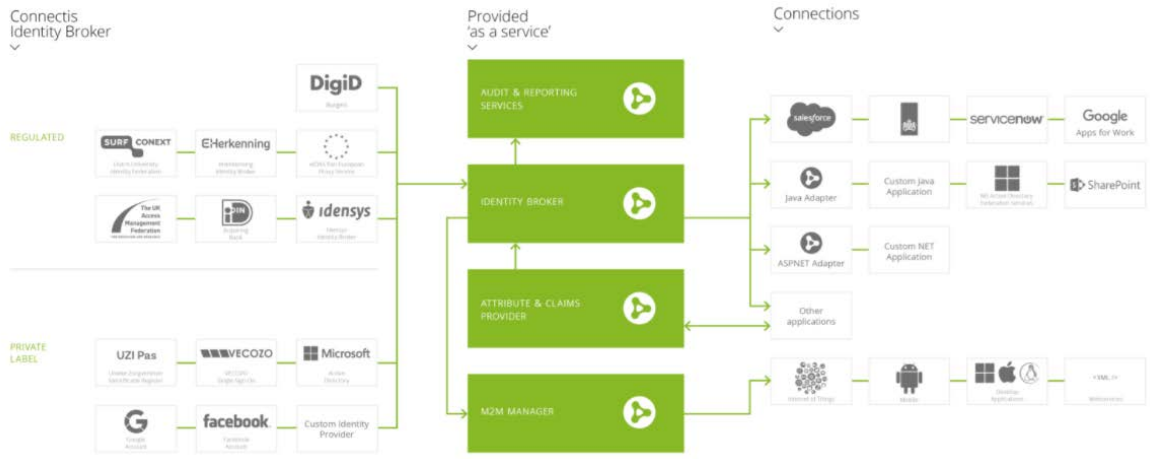

Figure 5: Broker offered by Connectis in The Netherlands

In Spain Safelayer has offering named TrustedX eIDAS Platform that is, according to them not brokering but "orchestrating" digital identities for authentication, electronic signature, single sign-on (SSO) and Two-factor Authentication (2FA) for Web environments[4].

When it comes to mobile operators and use of gateways or interfaces for mobile ID, Apigee Identity APIx is selected API-based solution that empowers mobile network operators using the GSMA Mobile Connect. It is offered as part of the GSMA Mobile Connect Accelerator (MCX) program and is also available as a cloud service in order to enable operators to increase scale rapidly. Other solutions for API management include IBM App Connect, Dell Boomi, Tibco Machery (bought by Intel), WSO2 API manager, Jitterbit, Azure API management, Axway, CA technologies (after it bought Layer 7), eScale etc. Not all of them are suitable for identity API management due to the security risks. Operating some of these from public cloud brings additional risks. Direct LDAP connectivity, for example, is generally considered a security risk so specialized identity API managers recommend a SAML SSO provider integration instead. Another vendor with focus on identity is Axway with experience in B2B federated identity management. As mentioned before, there are API management and API gateways integrated with identity management solutions. CA Identity Portfolio for example comprises many solutions such as Identity Management and Governance, Privileged Access Management, Single Sign-On, Advanced Authentication, and Directory products. The product can be deployed on-premise, but also as SaaS through partners. For authentication, CA Identity Portfolio includes social logins, KBA, and OTP (email, phone, and SMS). Third party authenticators interoperate with the platform while API gateway provides set of features for mobile scenarios, including device-to-back-end API authentication, device-level certificate management, single sign-on to multiple apps, and the ability to transfer user sessions across devices.

Pricing for identity APIs depends strongly on number of users, environments, number of API calls and number of reports requested, as well as requested support services or service level agreement (SLA). In a matter of fact, the most commercial providers offer SLA with the availability guaranteed to above 99,5% of time, which is probably the main obstacle if eIDAS APIs are to be operated by the government.

[4] https://www.safelayer.com/en/eidas-electronic-identity-authentication-signature

In general, when it comes to the trends analysis regarding eIDAS brokers we can envisage several scenarios where LEPS results could be exploited:

- Emergence of new specialized eIDAS brokers for specific groups of e-services, such as sectorial e-services, where sectorial association could play the role of operating eIDAS broker. This is likely to happen in some sectors, such as education, where organisations such as GEANT already has some experience in managing different e-ID services, such as eduroam or edugain. In LEPS some actions have been taken to check the feasibility of this approach for postal sector, through external stakeholders such as UPU and PostEurop.
- Addition of eIDAS brokerage to the existing identity brokers, including already established CIAM. This is likely to happen in the case of EU based CIAM providers and identity brokers, such as Ubisecure, Safelayer or cloud-delivered eIDAS as a service from SkIDentity. These solutions are not sector or service provider specific, but are likely to be more attractive for e-service providers that need more versatile eID options (with different assurance and privacy levels) and need to offer several options in parallel before making full migration to eIDAS eID services.

3.2 Adoption of e-IDs among e-service providers

There are many sources related to Identity & Access Management Market predictions. Some of them are making segmentations (Provisioning, Directory Services, Password Management, SSO, Audit, Compliance, Governance etc), while the others provide figures per sector. Report [8] on overall identity & access management market estimates growth from USD 8.09 Billion in 2016 to USD 14.82 Billion by 2021, at a CAGR of 12.9% between 2016 and 2021. According to another analyst, Stratistics MRC, the Global Identity & Access Management market is estimated for $7.94 billion in 2016 and is expected to reach $20.87 billion by 2022 growing at a CAGR of 14.8% during the forecast period 2016 to 2022. Regardless of these high-level figures, all analysts agree that growth is higher than in the most It segment and this is especially true for mobile ID. Given that users in LEPS are operating in postal and financial sector, in this analyses we focus on suitability of eIDAS eID services for adoption by e-services in postal and financial sector.

Externalization of eID services is now common practice for any e-service operator. We did research on different motivations that lead e-service provider move to integrate external authentication. The research was based on various market analyst reports (Gartner, Forrester) as well as internal survey among Atos clients. One of the most important issues reported by almost 50% of e-service providers is the cost of administering the internal authentication system, followed by other issues such as need to make constant evolution to the eID solution (scale, multi-channel access, new protocols etc). While the motivation for adoption of external eID services is mainly cost, compliance and security are mentioned as the main drivers for abandoning social logins that rely on self-assured identity, passwords and even traditional two-factor authentication (2FA) solutions.

3.2.1 Postal sector

The EU postal sector accounts for €91 billion or 0.72% of EU GDP[5] but the traditional mail market is undergoing a strong structural transformation due to digitization. Today 60% of Posts say they can make money from selling digital services (source: UPU) with e-post services such as e-cards, electronic notification, or hybrid mail.

[5] the European Commission has been collecting data on postal services in cooperation with the Postal National Regulatory Authorities (NRAs) of participating countries in the context of the 'EU Postal Survey' (http://ec.europa.eu/growth/sectors/postal-services/statistics_en)

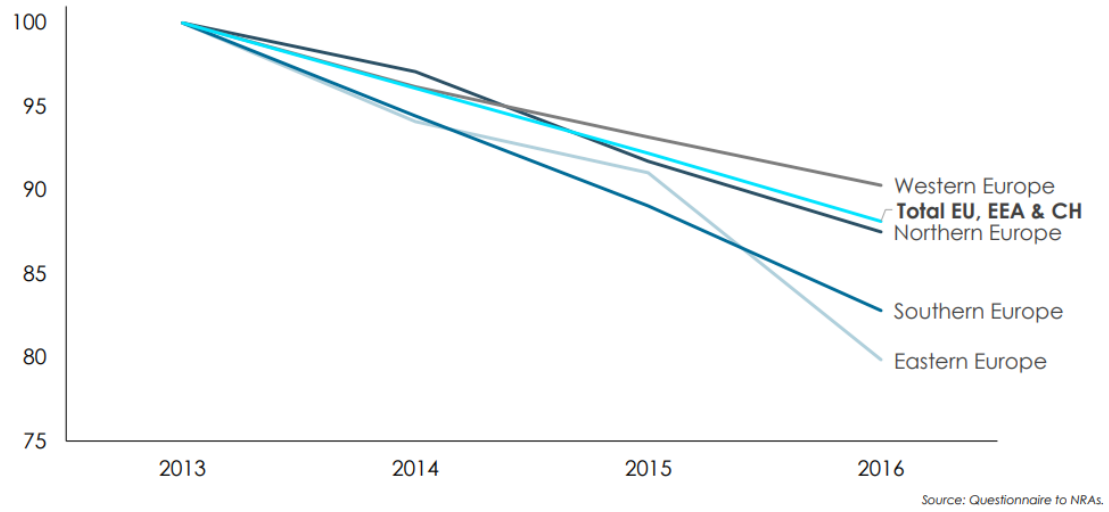

Figure 6: Evolution of mail based services in EU postal sector

In a study made by Copenhagen Business School, graph is made with data from the last 4 years (see figure above) with the countries such as Denmark, Netherlands and Italy as countries with the highest decline. In contrast to mail, parcel delivery was found growing (see figure below).

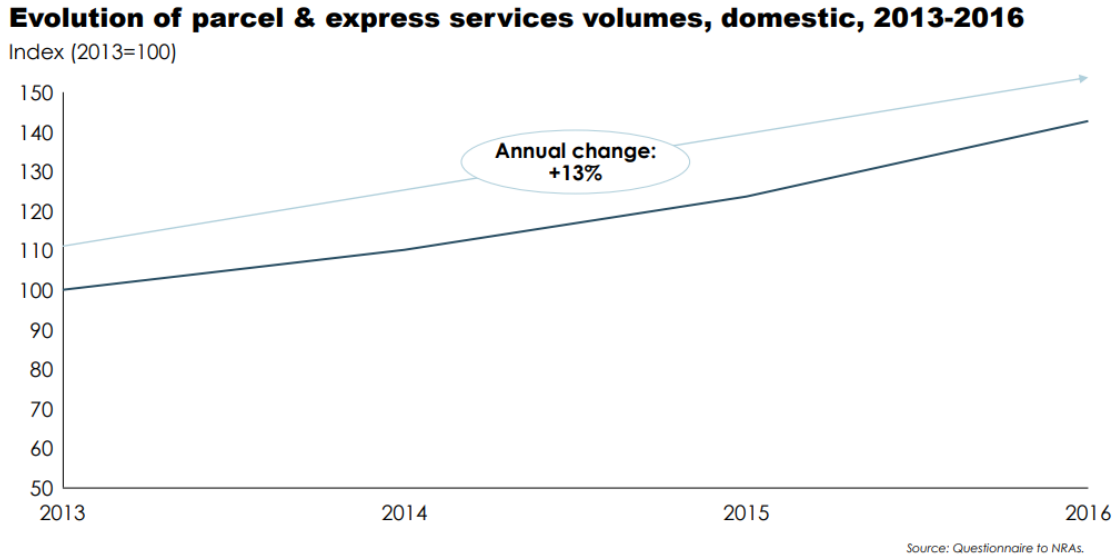

Figure 7: Evolution of parcel and express delivery services in EU

The origin-destination of parcel delivery varies in the case of each country. For UK, for example, the most deliveries comes from China (38% of all cross-border parcel deliveries) while for Austria the main source is Germany with 78%. However, the competition is much higher in this sector with new express mail and parcel delivery companies appearing on the market. Besides this study, similar findings can be found in Austrian study[6] or Dutch NL Post study[7].

The parcel sector is especially important segment for cross-border e-commerce. Over 6.4 billion items were shipped in 2011, and as the EU states "the cost and efficiency of parcel delivery should not be an

[6] https://www.post.at/gb2009/en/Postmarkt_Europa.php
[7] https://www.postnl.nl/en/about-postnl/about-us/market-and-regulation/research-on-the-european-postal-market/

obstacle to cross-border e-commerce". Many of the current online services provided by postal sector operators refer to track and trace (90% of e-post implemented this) and online information on services and tariffs (83%), which do not necessarily need or rely on e-ID services. However, services that were also considered by LEPS, such as "online philatelic and postal products shop" and "electronic remittances" directly generate revenue for Posts and could be candidates for connectivity to eIDAS infrastructure since these are cross-border services by its nature. Postal electronic mailbox, such as the one from LEPS pilot, is implemented in 33% of countries and has the highest growth rate, while emerging services in some countries include integration of postal web services with external services such as e-merchants sites, payment solutions or online customs declaration. On 25 May 2016 the Commission adopted a proposal for a Regulation on cross-border parcel delivery services, as part of a package of measures to allow consumers and companies to buy and sell products and services online more easily and confidently across the EU. In order to limit the administrative burden, for example, the transfer of data by parcel delivery providers, national regulatory authorities and the Commission should be electronic, for example by allowing the use of e-signatures in line with the eIDAS Regulation. If we look at statistics provided by EU DG Internal Market, Industry, Entrepreneurship and SMEs, number of international (so cross-border but not limited to EU member states) traffic in parcel delivery and express services, Greece and Spain are among the countries with the highest cross-border traffic, probably due the fact that they are tourist countries (same as Croatia, for example, which also has very high indicator).

The 2017 IPC Cross-Border E-Commerce Shopper Survey [22] mentions three-quarters (74%) of respondents had a parcel delivered to their home in the past year. A quarter (26%) picked a parcel up from a Post Office, 19% from a postal service point, 16% from a courier's parcel shop, and 16% had a parcel delivered to their office / workplace. When asked about identification and signature preferences, 31% of respondents said that they prefer to sign for all of their parcels, while a fifth said that they preferred delivery methods that remove the need for signature (e.g. delivery directly into their mailbox, which was preferred among younger respondents).

In regard to all topics related to postal e-services, LEPS project has already active experts in its industry monitoring board, namely from UPU (Universal Postal Union) and is also in contact with the project "Development of Cross-border E-commerce through Efficient Parcel Delivery" that was contracted to WIK Consult by DG GROW.

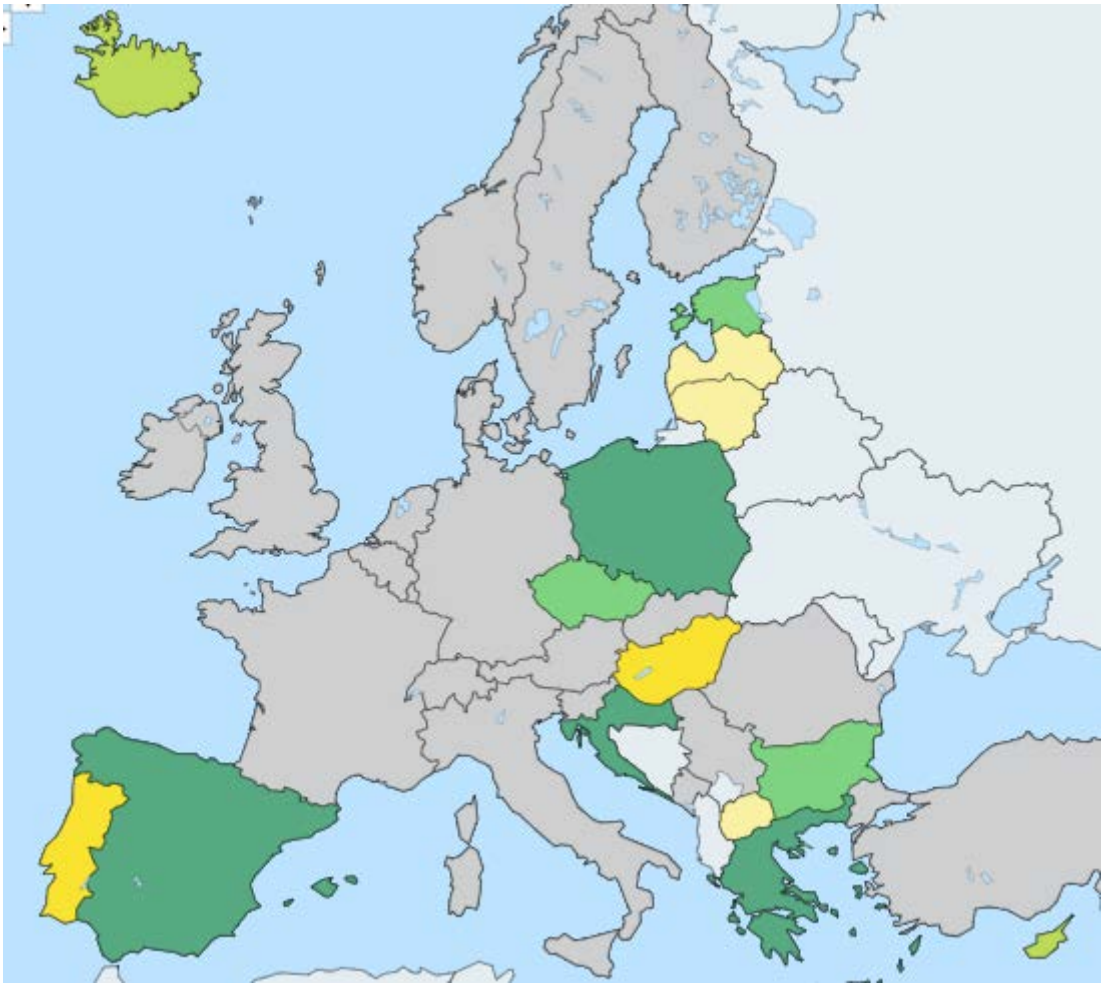

Figure 8: International postal traffic in 2016 – courier express and parcel delivery

Postal sector operator are not only service provider, but sometimes they also act as identity provider or, more frequently, as identity verification provider. These services are leveraging on trust in the postal operator, as well as proximity, however, adoption of Postal e-ID solutions remains low with digital identity used only in 22% of cases, according to the study done by UPU [9]. During the last few years, the postal sector has developed a framework of e-ID related postal products which can be found in the UPU "List of e-post and e-government services" (see figure 8, dark green – the highest number reported, light yellow – smallest number, grey – no data available).

In [24] several examples (Australia Post, Poste Italiane, Denmark Post, and Swiss Post) are outlined as examples of trust-based that are expected to introduce applications targeting new segments (such as e-health) and to extend their platforms to new sets of personal data (such as those generated by "smart cities").

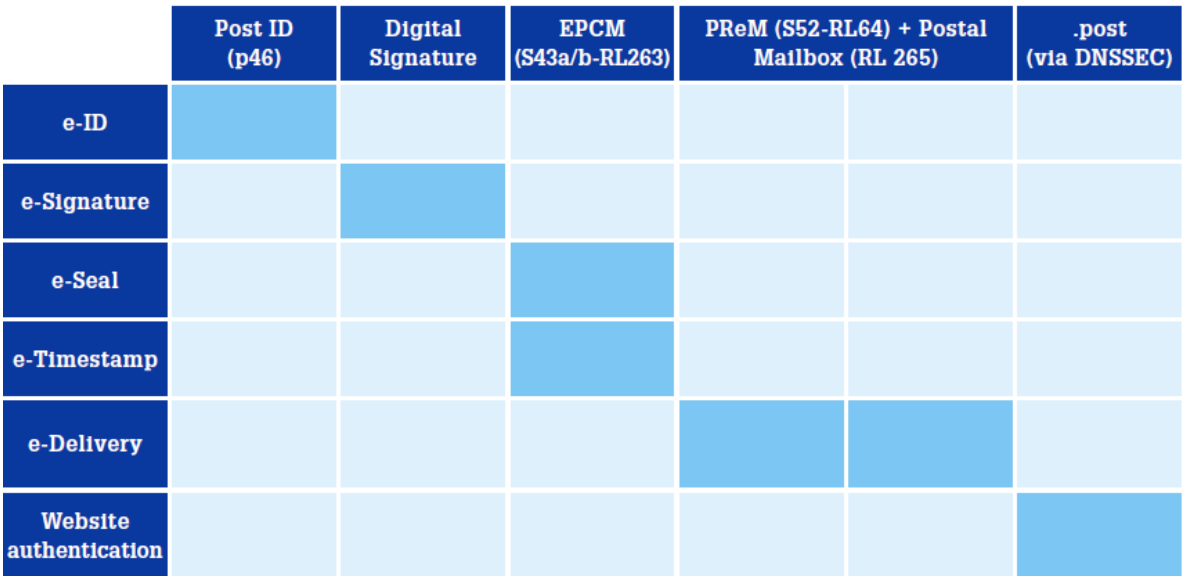

Figure 9: Offering of postal products related to e-ID (Source: UPU)

In Switzerland, Swiss Post finished a pilot project in 2017 with 3,000 customers to integrate a SwissID into their customer login. Sometime later, they have decided to work together with other sectors to create a trusted Swiss brand for e-ID, endorsed and certified by government. The companies involved are Swiss Post, SBB, Swisscom, Credit Suisse, Raiffeisen, UBS, ZürcherKantonalbank, financial services providerSIX and Schweizerische Mobiliar. Newcompany, SwissSign Group AG, will integrate the activities of existing firm SwissSign AG from January 2018, and continue to develop the "SwissID" solution.

Similar occurs in Germany where companies (including Allianz, Daimler, Deutsche Bank with Postbank) have joined venture called Verimi. German PostID has already expanded a number of identity verification means including face to face (in person), by German National eID card, by chat or by foto. Deutsche Post is not "notified eID provider", but in the future we can also envisage situation where cross-border identity verification infrastructure, similar to eIDAS, is targeting "national identity verification operators", where the solution such as the German Post ID could play an important role.

Poste Italiane recently launched Poste ID, a mobile-ready, secure identity management service. The service emerged from its experience offering individual services for specific functions of government bodies such as police or tax authorities, and the realization that it was well-positioned to offer a platform to support multiple online services, including government affairs. In a matter of fact, Poste Italiane is a Qualified Trust Service Provider according to Regulation (EU) N.910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) authorized by AgID (Agenzia per l'Italia Digitale), the Italian supervisory body that grants qualified status to trust service providers. Poste Italiane uses the PosteID system on its own e-commerce website, postshop.it, and the payment app Postepay. In addition to access and payment capabilities, it will offer the ability to sign electronic documents by clicking on the PosteID button on a webpage and entering the code sent from the App.

Finally, different role of postal service operator in national eID schemes are exemplified by La Poste in France and Post Office in UK, that participate as identity providers in national schemes (France Connect and Gov.UK Verify), but compete with the other identity providers.

Outside of Europe, Australia post started to use derived or so called "virtual" identities. As from January 2018 any citizen can submit the document details needed to create an entry level ID (driver's license, passport, Medicare card for example) online or via a smartphone app. In order to complete the biometric component iPhone users will need to visit a Post Office where a photo license or passport can be sighted, while Android smartphone users who have an NFC chip in their phone can skip this step and simply use the NFC card to read the chip in a recent passport to make biometric verification.

3.2.1.1 Strategic positioning of postal service operators

We have already mentioned two features that put postal service operator in a rather unique position, positioned somewhere between retail banking and governmental sector: trust and proximity.

In Figure 16 that was taken from [23] the unique positioning of postal sector regarding different service sectors and social capital (like trust and proximity) is depicted.

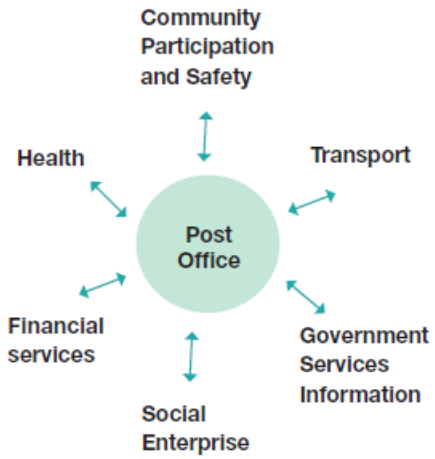

Figure 10: Post office between social capital and enterprise

We have also mentioned that many posts have pursued the development and integration of e-services. Digital mailboxes (or e-boxes) are example of service positioned as essential for secure, authenticated digital transactional mail communication between government or utility service companies and citizen. The technical infrastructure enables senders (usually businesses and governments with large mailing lists) to manage critical and time-sensitive, document-based communication and multimedia message distribution, while meeting individual receivers' needs for a centralized space for the management and archive of transactional communication. For businesses and governments, it offers an innovative way to use technology to simplify workflows and conduct essential transactions more competitively, without compromising customer service [19].

While online post services exist already for a number of years, some operators are now using mobile technologies to raise the bar of postal convenience for customers on the move. In 2011, Post Denmark launched MobilPorto, a mobile postage app that won the Postal Technology International Delivery Innovation of the Year award that year. The MobilPorto postage app acts as a mobile franking service. Customers can use the app to gain access to a unique number, which is written on a letter and acts as a stamp [28].

Finally, as one of the most important developments in the postal sector, we should mention that in 2012 UPU launched ".post" (dotpost) platform, a top-level domain for the postal sector. The platform's goal is to interconnect current and future electronic postal services and make them interoperable in a secure and trusted environment. It will authenticate postal service providers and strengthen the postal brand globally. ".post" intends to link the physical and digital worlds, creating a secure platform that enables postal e-services [29].

3.2.1.2 Cross-border postal e-services

Cross-border mobility is one of the main objectives of the EU eGovernment Action Plan 2016-2020 and represents an important milestone towards realising the Digital Single Market. Achieving cross-border mobility across Europe will on the one hand offer more opportunities for citizens to work, live, and study in any European country; on the other hand it will enable businesses to set up shop anywhere across Europe, thus boosting Europe's attractiveness and competitiveness as location to invest and conduct business in [20].

In regard to cross-border services, or postal e-services offered to foreign residents, online information is the most used one, while track and trace comes rather close. Online philatelic and postal product shop is implemented in 27 countries with interfaces that target foreign or cross-border customers, while this is the case for 10 operators for e-mailbox service. As an intermediator for government services (e.g. before mentioned e-mailbox service) postal sector is well positioned to address needs of accessing foreign citizens, for example those that have property in one and live large period of time in another member state (e.g. senior citizens). They could receive government notification to their e-mailbox independently from the physical address. In a matter of fact, government agency services can account for up to 15% of posts' annual revenue. Trust among businesses and consumers is among the core competencies of postal operators and provides an opportunity for building a range of e-government services. Trust forms a significant part of e-government uptake, with citizens' concerns often centering on data integrity and security. Digital identity services (including identity verification) are the second-most common e-government service offered by posts after digital mailboxes. They allow citizens to access a wide range of e-government services, including those traditionally available through postal retail outlets, including tax return filing and vehicle registrations. In offering a portal to access these services, posts can maintain strong ties with trusted government services. Poste Italiane, for example, manages the whole process of certifying Italian citizen electronic identity, using its own physical (14,000 post offices) and digital (cyber security centre) assets.

A study conducted by UPU[8] indicated that:

1. **Postal e-services are growing globally, but there is a divide between industrialized and developing countries**
2. **Innovation capability influences the development of postal e-services more than wealth does. The e-services strategy, management and profits are still not aligned**
3. **UPU has allocated e-services into 29 categories.**

Specifically, across EU, 29 ePost services have been offered by national postal operators.

The following table depicts the various e-Postal services (green colored rows represent web services that will be developed in the context of LEPS – eDelivery services by ELTA).

[8] "Measuring postal e-services development" - A global perspective, UPU

UPU Code	Service	Description	ELTA	Austrian Post	Nord Post	LaPoste	Deutsche Post	Post Itanlane	PPT	Correos	SwissPost
101	**Public Internet access point in post offices**	Customers can access Internet services in post offices.							X		
102	**Web information on services and tariffs**	Customers can access information about the different services and products, as well as the corresponding tariffs, on the Post's website.	X	X	X	X	X	X	X	X	X
103	**Postal electronic mailbox**	Enables the sending of electronic messages by an authenticated mailer and the delivery and storage of electronic messages and information for the authenticated addressee. Defined in article 14 of the UPU Convention and article RL 256ter of the Letter Post Regulations.				X		X	X	X	X
104	**Online direct mail**	Delivery of advertising and/or other promotional communications by the Post via electronic means.			X	X	X				X
105	**Postal registered electronic mail**	A secure postal e-service that provides proof of sending and proof of delivery of an electronic message and a secure communication channel to the authenticated users. Defined in article 14 of the UPU Convention and article RL 256bis of the Letter Post Regulations. A draft UPU functional specification standard (S52) exists.	X	X		X	X	X		X	X
106	**Electronic stamp**	Postage that has been electronically paid for and downloaded, for instance through the Post's website or a smartphone application. The postage is then printed physically or stored electronically. It constitutes proof of the prepayment of the value of a postal service. Usually, electronic stamps take the form of a barcode or an RFID tag.				X	X			X	X
107	**Customized electronic stamps**	Electronic stamps designed according to the customer's needs and preferences. For instance, the sender may		X		X	X		X	X	X

		incorporate a personal image in the stamp.									
108	**Electronic postal certification mark**	Provides evidentiary proof of an electronic event, in a given form, at a given time, and involving one or more parties. Defined in article 14 of the UPU Convention and article RL 256 of the Letter Post Regulations. A draft UPU functional specification standard (S43) supports this service.				X			X	X	
109	**Electronic signature**	Provides the possibility of digitally signing documents.		X		X	X	X		X	X
110	**E-telegram**	Provides the ability to compose a telegram electronically, such as by e-mail or SMS, with the telegram being delivered to the recipient physically				X		X		X	
111	**E-cards**	Provides the ability to buy a postcard online, which is then delivered to recipients by physical or electronic means.		X	X				X	X	X
112	**Online burofax**	Permits the transmission of texts and illustrations true to the original by fax, as defined in article RL 254 of the Letter Post Regulations								X	
113	**Hybrid mail (electronic to physical)**	Enables customers to send an original message, which is then processed electronically and converted into a letter-post item for physical delivery to the addressee. Defined in article RL 253 of the Letter Post Regulations.	X	X	X	X	X	X	X	X	X
114	**Hybrid mail (physical to electronic)**	Enables customers to send an original physical message, which is converted into an electronic form for delivery to the addressee. Defined in article RL 253 of the Letter Post Regulations.		X	X	X		X	X		X
115	**Postcode lookup**	Enables customers to find a postcode online by entering information such as an address, a company name or a city.	X	X	X	X	X	X	X	X	X
116	**Postal address validation**	Enables customers to verify an address by entering it online to check against a database of valid street addresses and/or determine an area of uncertainty	X	X	X	X	X		X	X	X
117	**Post office location lookup**	Enables customers to search for the address of a post office online by entering information such as the street, the city or the	X	X	X	X	X	X	X	X	X

		postcode. Customers can also obtain additional information about the different products and services provided at the post office as well as its business hours.									
118	**Address change online**	Enables customers to change their mailing address electronically, including through an Internet portal.		X	X	X	X	X			X
119	**Holding of mail delivery online**	Enables customers to request, by e-mail, online application or phone, the suspension of mail deliveries to their address and the holding of their mail for a period of time.		X	X	X	X	X			X
120	**Track and trace**	Enables customers to electronically track and trace a postal item.	X	X	X	X	X	X	X	X	X
121	**Electronic notification to Post of letter needing to be collected**	Customers are able to notify the postal operator electronically (e.g. by SMS text message or e-mail) about a letter item to be collected from a specific physical address.				X		X			
122	**Electronic notification to addressee that letter is to be delivered**	The Post notifies an addressee electronically (e.g. by SMS or e-mail) about a letter item to be delivered to a specific address.			X						
123	**Electronic notification to sender that letter has been delivered**	The Post notifies a sender electronically (e.g. by SMS or e-mail) that a letter item has been delivered to a specific address.	X		X	X		X	X		
124	**Electronic notification to Post that parcel needs to be collected**	Customers notify the Post electronically (e.g. by SMS or e-mail) of a parcel item whose collection from a specific physical address is requested.	X					X			X
125	**Electronic notification to addressee that parcel is to be delivered**	The Post notifies an addressee electronically (e.g. by SMS or e-mail) of a parcel item to be delivered to a specific address		X	X	X	X			X	X
126	**Electronic notification to sender that parcel has been delivered**	The Post notifies the sender electronically (e.g. by SMS or e-mail) that a parcel item has been delivered to a specific address.		X	X	X	X			X	X
127	**Check mailbox contents online**	Enables customers to check the content of their physical mailbox by receiving an electronic version of their			X	X			X		X

		letters or by receiving electronic notification from the Post of new parcels.									
128	**Web-based customer service and contact**	Allow customers to contact the Post electronically for a service or information, via a website, e-mail or telephone.		X	X	X	X	X	X	X	X
129	**Applications on mobile devices**	Services provided by Posts through smartphone applications.		X	X	X	X	X	X		X

Table 2: Postal e-services: comparison between EU operators

It should be clarified that the eDelivery module of ELTA combines features of UPU "electronic inbox" and "hybrid mail". It will allow users to register via eIDAS and authenticate themselves. By the compeltion of the registration/login process they will apply for any document they wish to receive from Public Authorites. This application will be sent via e-Delivery (from the Access Point of ELTA to the Access Point of Citizens' Service Points a.k.a KEP). After the issuance of the certification, the document will be sent via the e-Delivery system to the Document Management system of ELTA and it will be added to the inbox of the users where they will be able to safely retrieve it. This process is rough equivalent of UPU "electronic inbox". If the recipient of the document is not part of the e-Delivery network, a physical message will be sent to him/her containing the url through which he/she will be able to download it or alternatively the document could be delivered in physical form (through a traditional postman delivery). This part of ELTA service is equivalent to hybrid mail service that turns electronic data into physical documents, delivered by postman to customers/citizens, as well as reverse hybrid mail that turns physical documents turn into digital files delivered via secure e-mail.

In addition to e-postal services, UPU is also listing e-commerce services offered by postal service operator, as an essential part of digital strategy for organisations from this sector. E-commerce services consist of buying and selling products and services using ICTs. It involves processing and delivering purchased items physically or electronically and, such as in case of postal sector operators, it is often focused on niche markets or products.

According to UPU, the six (6) codified e-commerce services provided by postal operators are presented in the below table (green colored rows represent web services that will be developed by ELTA in the context of LEPS – e Commerce services):

UPU Code	Service	Description	ELTA	Austrian Post	Nord Post	LaPoste	Deutsche Post	Post Itanlane	PPT	Correos	SwissPost
301	Online shop for philatelic products	Customers can purchase philatelic products online and have them delivered to a physical address.	X	X	X	X	X	X	X	X	X
302	Online shop for postal goods	Customers can purchase postal goods online and have them delivered to a physical address.		X	X	X	X	X	X		X

303	Online shop for non-postal goods	Customers can purchase non-postal goods online and have them delivered to a physical address.		X			X	X	X	X	X
304	Subscription for periodicals	Customers can subscribe to periodicals online and have them delivered to a physical address.		X	X		X				X
305	E-commerce web-based customer service and contact	A service providing the customer with an electronic online account and a unique contact identifier to manage and trace operations related to an e-commerce transaction		X	X	X	X	X		X	X
306	SSL web certificates	The Post issues SSL certificates for securing websites.						X			X

Table 3: E-commerce services offered by postal sector operators

3.2.1.3 Cross-border use of postal e-mailbox

In Denmark, the Danish Public Digital Post gives to authorities the ability to send digital-only messages, letters, documents to all Danish citizens and businesses. According to the Danish Public Digital Post Act, public authorities are entitled to send digital only messages rather than sending paper-based letters, with equal status and effect. In order to access the Digital Post, user must log on with the digital signature NemID. This implements a single login for public websites, online banking and many other websites and services. Users of NemID are assigned a unique ID number. It is used as a username in addition to their CPR-Number (the Danish Personal Identification number) or a user-defined username. About. 4,3 million Danish citizens and 680.000 businesses use and receive Digital Post today. Approximatively 400 national public authorities are part of the solution and send Digital Post messages via the solution. The volume of exchanged messages increased the last years. From 48 million messages in 2014, the figure passed to 86 million in 2015 and reached 71.5 million in 2016 (as of 1st September)9. As mentioned in [12] the CPR-nummer is considered data to be protected. It can be sent to Danish, national public authorities, but not for cross-border services. It is also discussed whether Swedish personnummer can be used across borders, or use of an alias is needed. STORK Deliverable D2.2 seems to claim that cross-border use is possible, at least with the consent of the person. Similar situation is with Iceland, while for Norwegian Fødselsnummer the conclusion is that is not confidential but it can only be used when there is a documented need. For this reason the cross-border personal identifier number is considered [12], likely as a sort of derivation through mapping algorithm or similar. Given national person identifiers, the Nordic countries should be close to defining a service or region specific eIDAS minimum data set.

[9] (https://joinup.ec.europa.eu/document/denmark-improves-user-experience-its-digital-post-solution-skat-nemid)

3.2.1.4 Cross border use of online Zip Codes for business users

Deutsche Post has created a comprehensive and up-to-date web based street directory. The directory, which is based on original Deutsche Post postal data, provides access to more than 1.2 million street names. What's more, it also contains information on postal codes, towns/cities, and municipality keys from the Federal Statistical Office. This means that accurate postal addresses can be incorporated into customer's systems and that postal addresses throughout Germany can be checked for postal correctness, and linked to other information as early on as the collation process.

Further to that, DP has developed a specific web service, based on zip code and other GIS information, called the " microdialog" which allows entrepreneurs to find out more about their existing or potential customers' profiles and identify new market opportunities (socio-demographic and consumer information, structural characteristics, regional data, information on private customer behavior in the insurance, banking and financial markets as well as information on private car ownership.

Moreover, UPU - Universal Postal Union has already designed and promoted a world postcode database containing the postcodes of 192 member countries. By using the POST*CODE® DataBase users has the ability to look up, validate, cleanse or customize (by geographical region or country) addresses worldwide.

3.2.2 Financial sector

There is traditional reluctance by financial sector e-service provides when it comes to use of government eIDs although innovative models have deployed in Nordic countries (endorsed eID such as BankID, combining data on top of government issued eIDs[10]). One of the main obstacles was around service level agreement and liability scenarios to minimize financial risks given the financial consequences can be very high for financial service providers if trusted IdP services are not available. However, a progressively emerging landscape for trustworthy remote identification, based on trust services for business value creation/business growth, better services for customers (differentiating value) and compliance with main EU policy initiatives (Know Your Customer policies - KYC, Payment Services - PSD2) and Anti-Money Laundering - AML) creates a new set of opportunities for introduction of eIDAS compliant eID services in financial sector, including the particular domain of cross-border financial transactions. Yet, sector specific rules i.e. face-to-face requirements for identification in banking as well as the legal obligation for the customer to provide a bank with a pen-and-paper signature, may currently introduce practical, operational, obstacles to uptake the use of cross-border eID services.

Generally speaking, the need to achieve greater operational efficiency and obtain additional business benefits from exploring new opportunities in the cross-border financial markets, introduce a certain "creative destruction" in the traditional identity management schemes and make digital onboarding particularly attractive. As a result, financial institutions are now more keen to build also on eIDAS interoperability and standards for cross-border use of e-identification and digital onboarding of customers in Europe, especially in the retail banking [17]. In this regard, banks should be able to rely

[10] For a short overview, of the Swedish eID system in particular, see in particular "Swediosh eID" available at: https://joinup.ec.europa.eu/document/swedish-eid-swedish-eid

upon eID means recognised at national level for domestic and, under the eIDAS framework, for cross-border access and transactions. eIDAS was included as a possible solution in the Green Paper on retail financial services[11], as well as in the European Banking Association (EBA) Discussion Paper on strong customer authentication and secure communication [13]. In a follow-up to the Green Paper specific measures will be put forward via an Action Plan and eID will be part of it.

Obviously, the stronger push towards cross-border banking based on digital electronic identification and trust comes from the European policies favoring the deepening of the European single market. The European Commission promotes a framework that stimulates the emergence of a single market for retail financial services (insurance, loans, payments, current and savings accounts and other retail investments), while in parallel applies concrete policies that facilitate the cross-border activity of European financial institutions such as: a) the Revised Payment Service Directive (PSD2) which implements an environment of increasing competition by letting third party providers of financial services build services on top of banks' data and infrastructure and operate in the whole EU market[12], b) the Fourth AML (Anti Money Laundering) Directive which defines new rules allowing merchants, including banks, to verify customers remotely using electronic means[13].

3.2.2.1 Current situation and enablers

The adoption of eIDAS Network authentication depends essentially on the perspective of increasing cross-border financial transactions. According to Eurobarometer study [15], one in 3 Europeans live in regions bordering other Member States and about 13.6 million EU citizens live in another EU Member State. However, only 7% of European consumers purchase at least one financial product or service, such as current bank account, credit card, car insurance, in another EU country. Less than one in twenty purchased their current bank account (3%), their savings account (1%) and their credit card, in another EU Member State; and, less than one in twenty respondents purchased their life insurance or their car insurance (1%) in another EU Member State. Of course, the younger the respondent, the more likely they are to have bought one of their financial products and services in another Member State (11% aged 15-24 vs. 5% of those aged 55+), according to [15].

[11] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:630:FIN
[12] EBF, PSD2 Guidance, available at https://www.betaalvereniging.nl/wp-content/uploads/EBF_PSD2_guidance_september2016.pdf
[13] A. Servida, 2016, eIDAS & 4th Anti-Money Laundering Directive - a short update, available at https://ec.europa.eu/futurium/en/content/eidas-and-proposal-amendment-4th-anti-money-laundering-directive

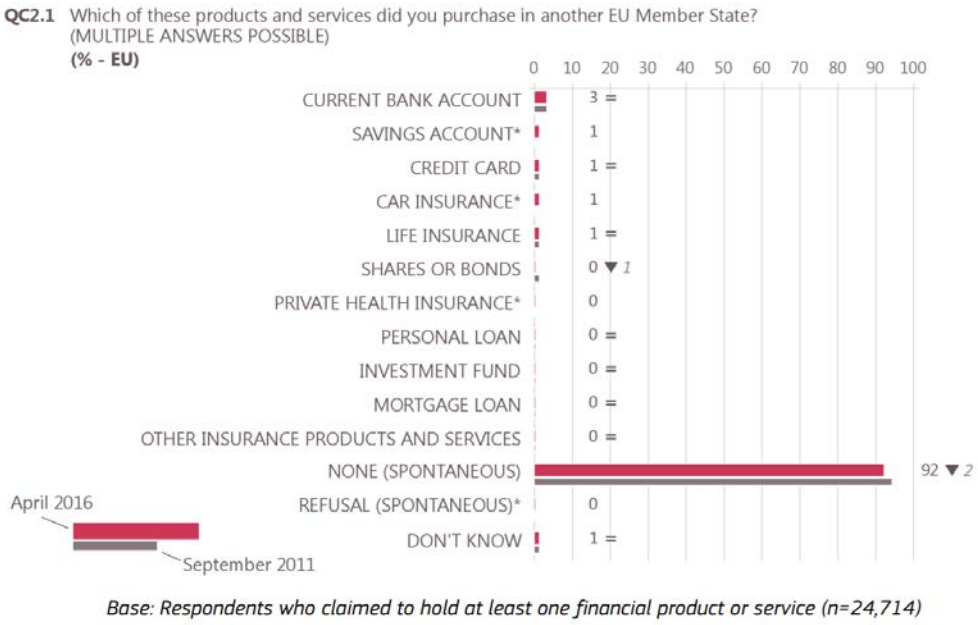

Figure 11: Cross-border use of financial products (Source: Eurobarometer 446)

Of course, the situation is different from the Luxemburg and Sweden to France and Greece, with consumers in the Nordic countries most likely being willing to buy financial products in other EU countries.

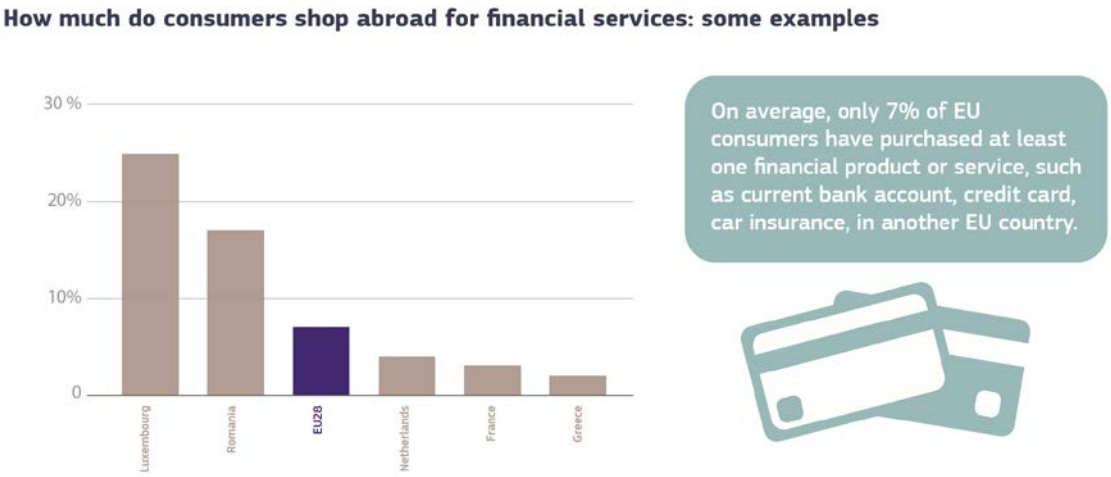

Figure 12: Use of cross-border financial products per country

In any case, as Eurobarometer documents explain *"the reasons why citizens do not buy financial products in other countries tend not to be tangible barriers such as language or consumer rights, rather it is the lack of perceived need or the perception that everything can be purchased at home"*[14].

[14] Eurobarometer 373, 2012, Retail Financial Services, available at https://data.europa.eu/euodp/data/dataset/S990_76_1_EBS373

Other friction forces apply at the level of financial providers, such as the application of EU law differently throughout Member States and the limited access to credit data information and consumer credit worthiness abroad. However, in order to make consumers able to access larger quantity of financial products available across EU, one of the key enablers is the use of e-ID services, in the framework of eIDAS regulation. In fact, the EC, in the recent *Consumer Financial Services Action Plan: Better Products, More Choice* [18], defines the cross-border use of electronic identification and the capacity of the banks to identify their customers digitally as one of the 12 Key Actions.

Electronic identification is a great opportunity but it is also a challenge. For banks and the other financial institutions, is essentially the key for extending identities that merge all identity sources (including biometrics" and exploit "analytics technologies during enrolment and authentication to increase insight and service relevance, while reducing fraud, waste and abuse" [16]. In such a perspective, LEPS has defined three important issues that should be considered in particular:

1. The creation and promotion of best practices

It is important to promote the use of eIDAS based identification by continuously diffusing information on successful ongoing implementations within banks and financial institutions and pilot-projects that have been implemented in the past years and created a base-reference for future developments (such as STORK 2.0 e-Banking Pilot)[15]. Since, the interest of banks focuses essentially on the Opening a Bank Account[16] case and the portability of KYC information, pilot and well established practices in these two areas should be actively promoted to create momentum.

2. The need to elevate identity assurance level

In the scope of PSD2 directive there is a question whether the eIDAS regulation might offer one (of possibly many) suitable solution on which PSPs could rely for ensuring strong authentication of payments, for protecting the confidentiality and the integrity of the payment service users' personalised security credentials.

Strong Customer Authentication (SCA) Procedure envisages authentication elements that include the Personalised Security Credentials (PSCs), i.e. the personalised features provided by the payment service provider to the PSU for the purposes of authentication, as well as devices and software used to generate or receive authentication codes that may either be provided by the payment service provider to the payment service user or possessed by the payment service user without being provided by the payment service provider.

For strong customer authentication, PSPs have to ensure that a valid combination of authentication elements, i.e. based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, results in the generation of an authentication code that is only accepted once by the PSP for the same PSU. For electronic remote payment transactions, PSPs have to ensure that a valid combination of authentication elements, as described above, results in the generation of an authentication code to the payer's PSP,

[15] https://www.eid-stork2.eu/pilots/ebanking/index.php/en/

[16] With reference to the case of Opening a Bank Account in EU, see in particular a recent synthesis report on the ongoing activity and the related policies, provided by Open Identity Exchange (available at oixuk.org/blog/2017/10/03/opening-a-bank-account-cross-borders-with-a-digital-id-pre-discovery-market-intelligence-report/

which is only accepted once for the same PSU and which is specific to the amount and payee agreed to by the payer when initiating the electronic remote payment transaction.

3. Use of Mobile eID in financial sector

Mobile ID provides online authentication based on digital certificates and digital signatures embedded in the SIM card (or by using other technology e.g. generated in the cloud, use of secure elements etc) of a mobile device. Mobile eID may offer the same security and better User eXperience as identification (since the logistical inefficiency related to the use of smart cards can be avoided). Mobile eID may emerge as a powerful substitute for current ad-hoc online authentication bank practices, replacing passwords and two-factors authentication via SMS. Essentially, it may used a security complement to all digital channels of an organization. Currently, Norway eventually presents the most well known case of a significant use of Mobile eID in the banking transactions[17].

3.2.2.2 Cross-border Remote e-signature service

ATHEX integrates the pre-activation procedure of Sign service with the eIDAS Network. To this end, the service will be customized to allow users with eID_EU to register automatically to the service. As a result, the users will not be requested to deliver the Subscriber Agreement together with a validated copy of their identity card, but to authenticate via eID_EU (with obvious benefits from both the users and the company).

In more details, an new customer of ATHEX Sign service has to visit the service web site and select "Apply Now with eID-EU" option. He/she will be next re-directed to "eIDAS Country e-Form" (where additional information on how to use eID-EU will be also provided). Upon successful completion of the authentication process, the User will be redirected back to the web site of the ATHEX Sign service in order to continue the online application process by filling a form. The fields "Family name", "First Name" and "Date of Birth" of the application form will be auto filled based on the values returned from the authentication process (via the eIDAS Network) – the User will not be allowed to modify these fields. ATHEX sign is currently used by 117 users.

3.2.2.3 Cross-border e-service related to information on investors position in central securities repository

ATHEX AXIAweb is the service providing information on the positions of an investor in the Greek Central Repository Group (https://www.axiaweb.gr/AXIAWeb/gr/login.htm). ATHEX integrates the AXIAweb service with the eIDAS Network. To this end, the service will be customized to allow users with eID_EU to register automatically to the service. As a result, the users will not be requested to deliver the Subscriber Agreement together with a validated copy of their identity card, but to authenticate via eID_EU (with obvious benefits from both the users and the company).

In more details, a new customer of ATHEX AXIAweb service has to visit the service web site and select "Sign-up with eID-EU" option. She will be next re-directed to "eIDAS Country e-Form" (where additional information on how to use eID-EU will be also provided). Upon successful completion of the authentication process, the User will be redirected back to the web site of the ATHEX AXIAweb site in order to continue the online application process by filling a form. The fields "Family name",

[17] https://www.gemalto.com/brochures-site/download-site/Documents/tel-cs-mobile-id-norway.pdf

"First Name" and "Date of Birth" of the application form will be auto filled based on the values returned from the authentication process (via the eIDAS Network) – the User will not be allowed to modify these fields. The user will have to fill-in only the fields "Father Name" and "Identification Document number" (e.g. Passport Number).

As soon as the user completes the fulfillment of the application form, a "Find my Portfolio" button will be activated. By clicking this button, the user allows ATHEX to search the database of Greek Stock Exchange Market if the User owns shares in the Greek Stock Exchange Market. If the search returns a positive result, a new user account will be automatically generated. Next, local credentials will be forwarded to the User via email or SMS.

By using eID_EU or local credentials, a registered User will be able to login AXIAweb site and review her portfolio in the Greek Stock Exchange Market ("Portfolio Access" page).

Currently there are over 6600 users of this service, from which 26 are cross-border users (the number is expected to grow in the future). This e-service, quite common to all stock markets, needs high level of assurance and is not available on mobile phone.

3.3 Policy context

In this chapter we briefly present main open issues when it comes to policy context around eIDAS regulation which should be mandatory around mid-2018. Additionally, to the specifications necessary for interoperability, the Implementing Acts of eIDAS regulation contain operational security requirements aimed at the operators of the interoperability components. The current state of discussions is to require operators to have an Information Security Management System according to ISO 27001 or equivalent national standards. The regulation also establishes a Cooperation Network of the Member States, i.e. a group where Member States can exchange information about their eID schemes. The main task of this Network is to perform the peer reviews as part of the pre-notification process, and to form an opinion on the schemes. Notification of an eID scheme involves several steps, including pre-notification, but at the time of writing this deliverable (March 2018) only Germany completed notification process, while Italy is in the stage of pre-notification.

The Commission (more precisely DG DIGIT) provides an open source implementation of the interoperability software and finances its deployment by the Member States, through the CEF (Connecting Europe Facility) program. The reference implementation is also used in LEPS project (and for this reason EUPL 1.2 license is selected for distribution of LEPS results). This software is based on the previous implementation of the STORK project, but at the moment it is not clear if other implementations will use it to achieve interoperability (according to the report from CEF website [2] only about a half of member states is reusing this software, as of March 2018). Every update of the reference implementation must be integrated in a new version and then deployed by all MS implementing it, which could be a limitation.

Currently the CEF DIGITAL WIKI is a collaborative space for Member States (closed community) addressed at eIDAS - eID implementors, eIDAS co-operation network, technical subgroup and governance. Moreover an open community in the CEF DIGITAL WIKI is addressed at eID users and service providers.

Currently special sub groups are working on user experience tackling issues related to the usability of eIDAS node and connected services. Last but not least a joint force for the use of eIDAS eID in the procedure of Know Your Customer, that is crucial for the banking sector, has been established.

The new EU GDPR regulation is entering into force the May 25th, 2018. It targets harmonization of individual's Data privacy rights for EU citizens. GDPR comprehensively applies to all organizations controlling and processing personal data of member states citizens and is enforcing a transparency for all European member states citizens with several opening clauses for country-specific provisions.

Sanctions & Fines applies pursuant to non-compliancy to the GDPR (ex. thief of unprotected personal data) administrative) fines up to 20 million EUR, or up to 4 % of the total worldwide annual turnover, whichever is higher (Article 83). There are other operational impacts that create an opportunity space for LEPS since Security/Privacy by Design should take into account the state of the art technology including high assurance of identity, and minimization of data sets used by service providers, in order to reinforce the security of personal data. LEPS related technologies to have in mind include data minimisation (article 5 of GDPR), data encryption, data integrity, confidentiality and availability, audit procedures and resilience, etc.

4 Feasibility and sustainability analysis

Cross-border and cross-sector interoperability is key to the growth of Digital Single Market and eID is clearly the main building block of it. Identification and authentication services are also at the heart of Digital transformation initiatives, innovative business processes and new generation of user experiences. According to the European Commission, a properly functioning digital single market could contribute €415 billion a year to the EU economy and create some 3.8 million jobs. The weight of eID in this is difficult to estimate, as many forms of low assurance eID are already widely used. However, the hesitation in adoption of higher assurance eID might result not only in decline of trust, but also in direct loss due to the identity related theft and fraud. In [11] for example, the potential value of a digital identity solution for Australia has been estimated to up to $11billion, saved through reduced cost to serve, cost of fraud and improved consumer experience. The same study, however, lists Sweden and Estonia as the best practice examples among high assurance e-ID ecosystems. The most interesting part of it is separating use of identity according to the frequency, which opens a door for a variety of possible solutions based on the risk for service provider, from separation of eID verification from eID authentication, to specific policy-based usage by service providers.

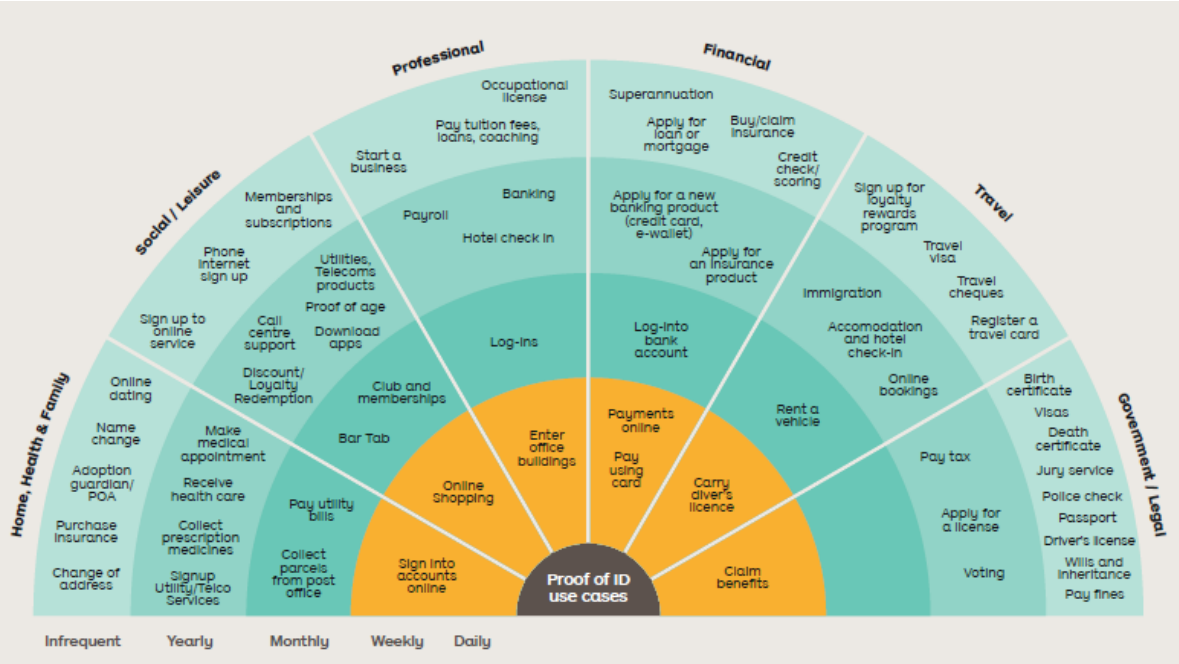

Figure 13: Use of identity (Source: Australian Post)

In the following chapters we present inputs for feasibility and sustainability analysis, as well draft business case for ELTA pilot that will be worked in more details in the deliverable D7.2, together with the other two pilots.

4.1 SWOT

SWOT analysis refers to strengths, weaknesses, opportunities and threats. It can be applied to a product, service, and an organization or even to a concept. In our case, it is a mix of all these, since the successful market uptake of notified e-ID across EU will depend on many issues, in which LEPS results represent only a small contribution. SWOT is therefore used as analytical framework that assesses what factors influence this e-Id adoption by private service providers, with the special emphasis on postal and financial sector. It this context the internal (the strengths and weaknesses) observations refer to LEPS results, but also to eIDAS context or e-services in postal and financial sector. In the same way, the external (the potential opportunities and threats) refer to other e-ID ecosystems and other private e-service sectors.

Strengths

- Political ambition to set a coherent agenda to promote the use of notified eID in EU (eIDAS Network) and in the private sector
- Growing internationalization of financial and postal service operators
- Combined EU and national investments in the development of eIDAS Network for cross-border recognition of notified e-ID in EU
- LEPS software available to make easier and cost effective integration of a Service Provider with the eIDAS Network
- Familiarization of e-services providers with the use of external identification services through API models (Facebook, Google, LinkedIn, Microsoft etc.)
- Strong position of postal sector operators as cross-border e-service providers connected to eIDAS, at the intersection between public and private, social and business, and, in some countries, acting already as identity provider and/or identity broker

Weaknesses

- The current level of cross-border use of e-services in the financial and postal sectors is rather low
- The “slow” pace of digitization in the postal sector (especially in the peripheral EU countries)
- The digital divide between EU countries that is reflected in differences regarding the available national eID services
- eIDAS Network and trusted services in the different EU countries is not at the same level of development
- The limited interest of e-service providers for high assurance eID services

Opportunities

- Increasing political and societal awareness of the multiple benefits related to the identification by electronic means
- The rise of cross-border e-commerce in all EU countries
- The momentum created by the number of pilot projects with notified eID in the private sector
- The irruption of mobile ID services
- The implementation of GDPR

- The rising societal and political concerns about the use of fake digital identities
- In the case of banking sector e-service providers, new anti-money laundering directive and know your customer might bring an opportunity regarding remote identity proofing and verification

Threats

- A certain reluctance in the private sector to use government operated or controlled e-ID services
- The inertia that may lead citizens to believe that "physical" identity verification is safer
- The over-publicity of every threat, vulnerability or "data leaking" episode
- Some identity brokers already have eIDAS connectivity feature for e-service providers, which is an opportunity for eIDAS adoption, but threat for LEPS results

4.2 Value Proposition

The value proposition that LEPS project result brings to the overall objective of maximizing eIDAS uptake in private sector is complex to define. The basic idea is that reusable software constructs, implemented integration and other intangible results (guidelines, experience) can contribute to eIDAS ecosystem and foster future private sector adoption of eIDAS. To cope with this challenge, the eIDAS ecosystem must remain highly adaptable, responding to the complex socio-economic context in which private online services are deployed.

On the other hand, uptake depends not only on service providers, but also on citizens that use these services. The process of feasibility and sustainability assessment has therefore to take into account desirability, feasibility and profitability (either financial or in terms of time) from all stakeholders involved in this multi-sided market. The essential characteristics are that eIDAS identity service integration (for service providers) and eIDAS eID services (for citizens) have to be:

- A desirable solution, one that both citizen and service provider really needs. The overall assumption is that in the age of rising cybersecurity threats, the higher level of assurance is not anymore optional, but a need. Different models for security technology acceptance have been discussed in [10] in regard to their application to e-identity and more specifically to national e-ID card. This includes Technology Acceptance Model (TAM) and Technology Threat Avoidance Theory (TTAT) related to avoiding security threats. Authors studied why the German eID is receiving little adoption as a privacy-preserving authentication technology, even though the technical capabilities are excellent. The conclusion, however, was that non-technical factors are necessary prerequisites for the wider adoption. In other words the higher level of assurance provided by connectivity to eIDAS ecosystem is simply not enough for the wide market uptake.
- A feasible solution, building on the strengths of operational capabilities. Given the investment in eIDAS done already, we can extrapolate some data and conclusions that would be applicable in the future for eIDAS IdP providers. In the case of service provider, data will be gathered from LEPS pilots and publicly available sources, but the focus will be to prove that replicability and reuse of components contributes to overall feasibility. In general terms we

can say that one of the main value propositions is related to low-cost integration with eIDAS eID services, thanks to LEPS components for service providers.

- A profitable solution, with a sustainable business model. Here again we have to take into account all stakeholders. While profitability for eID users is difficult to quantify (e.g. time spent for face to face identity verification), service providers have several alternatives models to calculate impact of eID services on their e-service business. The most common questions raised in this direction are, for example: How many users drops-off if eID services are too tedious, unsecure, privacy invasive etc? What is the cost saving due to the use of external eID services instead of internal solutions? How much cybersecurity cost can be avoided due to the use of preventive measures, such as high assurance e-ID? How many new users can be attracted thanks to the e-service integration with eID services from additional Idenity providers?

In the previous chapters we have discussed desirability from several angles, including the motivation to migrate to eIDAS e-ID services for services that need higher identity assurance or mobile ID. The issue of feasibility was addressed directly through LEPS results value proposition, while the issue of profitability, from service provider point of view, will be addressed in the next chapter with the simulation provided by ELTA.

4.3 ELTA business case analysis

In regard to the ELTA business case a simulation of revenue growth was done by ELTA. In 2017 in Greece almost 3,5 mn people purchased online goods and services worth of 4.5-5,0 bn €. In 2017 the ELTA corporate website (www.elta.gr) had 27,7 million visitors and 2,6 million registered users and the official ELTA Facebook page has 23.723 followers.

Approximately 7.000 SMEs are selling online and Greek citizens conduct 75% of their online purchases from them. Currently ELTA has aprx. 5.000 SMEs in its clientele data base in Greece. From these 5000 existing customers, ELTA targets 25% with its e-Delivery service, about 15% with Parcel delivery service and a similar rate for online zip code search for business users. Expected penetration rate for SMEs from other EU countries are lower, but given the high number of targeted market (about 50.000 European SMEs is registered as trading partner with Greece) the overall figure is rather high, with 1500 of cross-border SMEs being potential user of ELTA e-services. We should, however, take into account that parcel delivery voucher and online zip code search are existing services that will also support the use of existing eID (in parallel to the possibility to use eIDAS eiD services). These e-services are using low assurance level for identity services, so the main revenue growth is expected to come from e-delivery, which needs substantial assurance level and is a new service by ELTA.

Other possible users are Greek nationals living abroad and using some eId different than Greek. According to the General Secretariat for Greeks Abroad more than 5M citizens of Greek nationality live outside the Greek border, scattered in 140 countries of the world. The greater concentration have been noted in the US (3M), Europe (1M), Australia (0,7M), Canada (0,35M), Asia - Africa (0,1M) and Central and South America (0,06M). In this view as regards cross-European e-delivery our primary target will be on Europe (Aprx. 1M) with initial penetration rate set to 3%. Finally, for specific case of e-commerce and philatelists, the assumption is that from about 500 registered users some 15% (about 75) are cross-border users that will use this e-service.

ELTA first aim should be to focus on existing and new customers by pursuing 2 supplementary strategies: Revenue Growth and Market Share Strategies:

1. REVENUE GROWTH Strategy

1.1. Product Development Strategy: Promoting new e-services (eDelivery System) to existing customers (5.000 SMEs in Greece, penetration rate of the service → r>25%)

1.2. Market Penetration Strategy: Promoting existing e-services (compliant with eID features) to existing customers (penetration rate →25%>r>15%), focusing in particular to (a) registered users of the official ELTA website and Facebook page (2,6M). Projection will be based on the assumption that the penetration rate is expected to be between 15% and 25% (b) SMEs customers of ELTA in Greece (c) Philatelists 3.500 registered users in Greece, 500 registered users →350 from EU countries)

2. MARKET SHARE Strategy

2.1. Diversification Strategy: Promoting new e-services (eDelivery System, e-shop compliant with eID features) to new customers / citizens (penetration rate → 10%>r>3%, with special focus on (a) Greek nationals living abroad, (1M) projections will be based on a penetration rate 3% to 10% (b) e-commerce users (3,5M) projection will be based on a penetration rate 3% and 10%.

2.2. Market Development: Promoting existing e-services (compliant with eID features) to new customers (penetration rate → 15%>r>10%), focusing in particular to SMEs which represent (according to Hellenic Federation of Enterprises – a.k.a SEB), the majority (99%) of the Greek business community, counting around 700.000 business entities. Projection will be based on the assumption of a penetration rate between (10% and 15%)

The Adoption rate of 40% for the new and existing -compliant with eID- services, targeted to existing customers, are expected to be achieved in a 2-years period (strategies 1.1, 1.2)

Figure 14: Adoption rate of ELTA service according to revenue growth strategies

On the other hand, in the same time period (2-year), the adoption rate for strategies 2.1 and 2.2 for the new and existing -compliant with eID, services addressed to new customers, are expected to be of 16% to 20%

Figure 15: Adoption rate of ELTA service according to market share strategies

4.4 Sustainability plan

In chapter 4.2 we covered three characteristics that are essential for value proposition, as well as the sustainability. However, in regard to the sustainability there are many others :

- Organizational or governance approach on service provider side will depend on a number of services that each service provider wants to integrate with eIDAS eID services, as well as options such as sectorial "service provider hub".
- Evolution of user base – although number of EU citizens that have e-ID card is rising, the actual use of it is still low (although use of mobile ID, as already mentioned in chapter 3.1.2, is a promising trend). A special attention should be given to pioneers 8early adopters, influencers)
- Migration support – besides costs that will be treated in detail in deliverable D7.2, iterative and incremental approach was underpinned as important issue for sustainability, together with clear guidelines for service providers
- Identification of additional funding sources for early pilots
- Support from eIDAS node operator, with increased trust in the continuity of service, service level agreements, similar maturity level across all member states etc

The previous studies or projects already made several assessments regarding the sustainability of integration with eIDAS eID services. One of the more recent studies is [21] that analyses different options of e-ID service integration for the European Citizens' Initiative (ECI). Although integration of eID through connectivity with eIDAS seems more feasible from a technical point of view (integration with a single eIDAS node) and also seen as more secure (validation and extraction of the information contained in the eID certificates), the overall conclusion regarding maturity and other parameters are not very positive. In addition there are some legal obstacles (although applicable to the specificieties of ECI service).

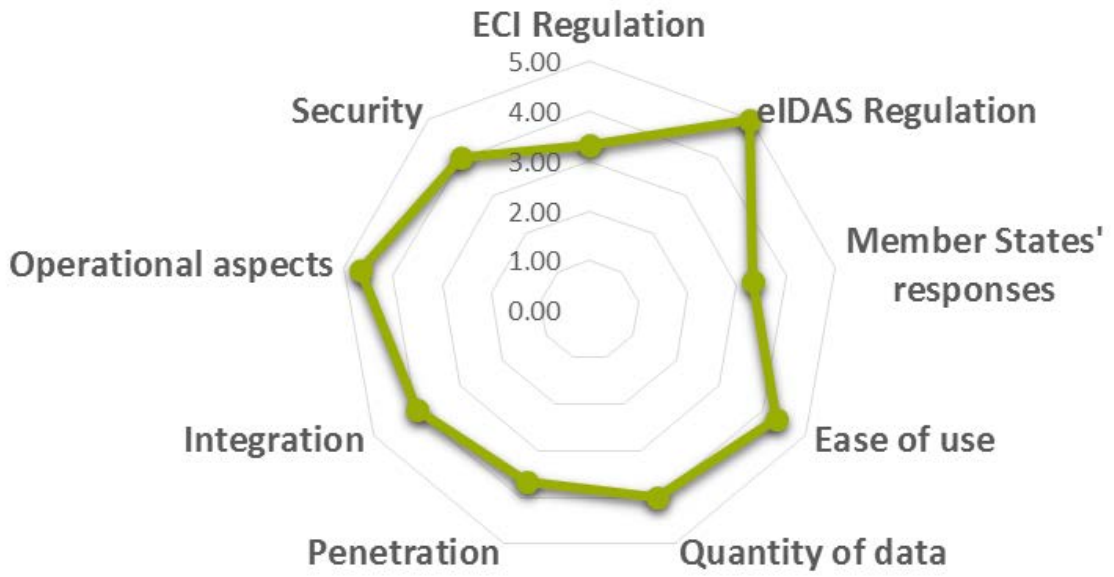

Figure 16: Assessment of eIDAS integration (Source: Everis)

The sustainability plans in LEPS consists of three main aspects, which are the current maturity of the building block, the possible future owners of the building block and the possible future actions to be taken. In LEPS technical maturity has been proven through successful pilots at three different sites. The ownership is clearly identified with EUPL licenses, which is in line with other CEF results. With respect to the type of actions that are proposed, we contacted several organisations in order to include LEPS results in their open source forge and enable reuse in the future by other actors.

Type of actions that are proposed is similar to the ones in other CEF Telecom building blocks, and we distinguish between the following:

- Define a new project for further development of LEPS results
- Put the result the forge for reuse in the future
- Make a link to the long-term sustainability communities defined in CEF
- Stimulate and act within the standardization community
- Involve stakeholders such as PostEurop or UPU to spread the word among postal community and use the results
- Involve companies that need to implement other elements, such as API management features
- Organize communication for adoption

We also envisage link to the long-term sustainability communities such as eIDAS cooperation network, PostEurop Innovation Forum (under the Operational Activities Circle (OAC) Working Group)) and FIWARE open community.

On April 4th Atos held conference call with FIWARE foundation and representatives of CEF-EID-FIWARE project[18] . the joint plan of action was agreed in order to publish generic enabler for FIWARE that would connect FIWARE IdM Keyrock to eIDAS in the first phase and later to any OAuth based IdM (similar to LEPS adapter). Asa founding member of FIWARE foundation Atos will provide full support and will promote this GE.

[18] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/cef-eid-fiware

In relation to the internal support for LEPS sustainability Atos made a number of actions to contact postal service sales community. In a webinar dedicated to cross-border e-commerce, LEPS was introduced and we expect that it could be used in commercial offerings as a kind of "added-value" plug-in for Atos clients. Additional presentations were made for sales support community (so called Digital factory department), as on April 20th, as well as for Public Sector community on April 23rd. feedback that was received was that there is a clear tendency for evolution of strong authentication in various sectors, not least due to the compliance issues regarding the remote identification. Implementation cost is not perceived as a major issue, in comparison to possible fear of user abandoning service.

Before the end of the project additional actions will be taken to involve more stakeholders to use the LEPS components. The focus will be on those that already have some experience with connectivity to eIDAS node. In a pilot between Netherlands, Belgium and Germany, for example, results were presented by Dutch Ministry of Economic affairs on the workshop held by EC on March 6th 2017, it was mentioned that service provider do have a business case, related to the traffic fine collection service.

A large-scale e-ID ecosystem around eIDAS is still to be created and it might be difficult at the present stage to envisage new roles of stakeholders such as identity brokers or trust frameworks. Single trust anchor, which is government in case of eIDAS, might be incapable of scaling beyond the boundaries of Europe or support the private sector adequately, so the alternative options, including identity proofing and verification (IPV) providers, endorsed identity providers etc might be also considered. It is likely that multiple eID ecosystems or schemes will co-exist and that service provider will have multiple options available for their customers.

We can therefore distinguish several scenarios in regard to the sustainable adoption of eIDAS eID services by private e-service providers:

1) All notified e-ID providers in eIDAS e-ID ecosystem come to an agreement to offer same level of support and similar resources for the ecosystem where eIDAS node operators would be the only intermediator in cross-border context between e-service providers and notified identity providers. As already notices in SWOT analysis, this option is unlikely given the situation in eIDAS adoption and implementation of national nodes is variable.
2) A subset of notified e-ID providers (e.g. "endorsed" by private e-service providers) is used as de facto standard for cross-border eID services. This is already happening at a regional scale (e.g. in Scandinavia) and at a national scale where there are multiple notified e-ID providers.
3) There is an emergence of e-ID brokers that also make agreements with some of notified e-ID service providers. Intermediation services in identity market are still in its infancy, but they will for sure need intimate relation and knowledge of the issuers as well as necessary technology to process the eID credentials (e.g. aggregate, transform, derive etc).
4) There is an emergence of IPV (remote identity proofing and verification) providers that focus only on the first phase if identity management and increase assurance regarding specific identification thanks to the technologies such as biometrics. These providers would address need of service providers related to face to face identity verification, which in principle is the most secure, but also the most costly both for service provider, as well as for citizen.

The last option is increasingly gaining attention. The UK good practice guide (GPG 45) provides guidance on the identity proofing and verification of individual using online services, while the EU is setting up the Commission expert group on electronic identification and remote Know Your-Customer Processes, mainly focused on financial sector. In the previously mentioned Mobile Connect

connection to French eIDAS node pilot, remote identity verification was tested by integrating mobile operator and government solutions via interoperable and decentralized layer based on API Exchange. The API Exchange is delivered by GSMA and it enables operators to federate between their individual APIs. APIs delivered by LEPS and listed in the chapter 2 could follow similar approach and we can think of sector specific “API exchange” solutions.

The EU can contribute to sustainability through several instruments. Traditional public procurement can be used to speed up the adoption, while some sort of Public Private Partnerships (PPPs), including the existing ones (e.g. ECSO or FIWARE) can be used to further raise awareness or disseminate good practices. Then there is the sector specific approach. This is already started in the financial sector, with the authentication and authorization of remote payments related to payment service directive (PSD2), or setting up of an expert group for the Know Your Customer (KYC) checks in the 4th Anti-Money Laundering Directive (4th AMLD). A similar effort could be done for postal service sector.

5 Conclusions

The first phase of LEPS project focused on customization of service provider e-services and preparation of reusable software components that enable eIDAS e-ID service integration. These components are listed and analyzed mainly from technological perspective, but the fact that LEPS provides three alternative architectural strategies offered a new way to look at their replicability and pan-European market perspective. Given the fact that the estimations of cost, in terms of effort needed for integration, customization and deployment of LEPS pilots, is not available yet (it will be summarized in D7.2), it is too early to make assumptions about the best alternative for e-service providers in general and LEPS pilot users in particular.

From the analysis of wider market trends related to eIDAS e-ID ecosystem and trends such as mobile ID or use of identity APIs, we can conclude that there is an increasing focus on hybrid approach in eID service provision, where the government issued eID are used to verify identities, while other private sector eID solutions are used for subsequent authentication services. The idea to elevate trust by using government issued e-ID for IPV services should not be confused with the elevation of assurance levels. Levels of assurance (LoA) contemplate the whole chain of identity lifecycle, from the breeder documents (birth registry) to the processes such as suspension, revocation or reissuing. The real challenge, therefore, seems to be related to the mapping and matching of these assurance levels that differ not only between member states, but also in the way these are determined for end to end identity lifecycle, now that different eID phases are being operated by different eID service providers. It is also interesting to observe market movements regarding the identity broker segment. In this segment we include all hubs, gateways, cloud-based multi-IdP solutions and similar that already provides support for e.g. multiple social logins. They are likely to enhance their IdP connectivity portfolio and become the main target for results such as LEPS software. However, generic-purpose brokers, including consumer identity and management (CIAM) solutions, are not trusted by many sectors and sector specific brokers, operated by sectorial association, might emerge.

It is clear that the business model behind eIDAS requires more attention and lessons learned from the previous national eID experiences should be taken into account. In some countries, such as Iceland, topic under discussion is whether government should charge for eID services related to high level of assurance. In other countries, such as Estonia, shift from mobile SIM card based ID towards mobile app based ID is opening a whole new range of possibilities. Third model is based on public private partnerships that proved to be successful in Scandinavia and are now also being started in Germany and Switzerland. Finally, there is also UK.Gov model with the multiple identity providers being accredited by the government. Among mobile operators, commercial federation service called Mobile Connect Link (MC Link) has been envisaged to exploit eIDAS opportunities.

In the light of these trends and initiatives, LEPS outcome is not and cannot be an isolated effort. Its sustainability relies on the partnership agreements and joint effort with the other partners, both private and public, with the special emphasis on the postal sector where the first contacts have already been established through PostEurop and UPU. In order to enable commercial use of eIDAS connectivity APIs, additional features need to be contemplated, such as dashboard with info on who is consuming which APIs, what is the traffic generated, was there any API downtime due to errors and timeouts etc. In a sense the problem is similar to the one already experienced by eIDAS node operators – in order

for eID services to be adopted the private e-service operators expect level of service similar to what they already experience with the other external IAM services providers.

When it comes to the postal sector, there are many additional possibilities, as described in market analyses of this deliverable. While some postal service operator are already established as eID providers, the others still have chance to put in place solutions that allows citizen a means of verifying their identity online based on government issued eID, especially for public e-services. Both postal and financial sector are tagged as primary target for early adoption of eIDAS eID services, but their starting positions and roadmaps are very different. Postal sector operators are still considered, in many countries, as "proximity services", often public or partially publicly owned, perceived as a kind of "social enterprise". They are already present in e-ID sector and many of them are likely to become "notified e-ID provider", therefore acting on both sides of eIDAS ecosystem. Financial e-service providers, on the other hand, already have long history and experience of operating their own eID services and trust frameworks. The possible scenarios in this sector are more complex and vary from Scandinavian model (banking sector operates notified eID) to a limitation of use of eIDAS eID to the first phase of identity management, which is so called "digital onboarding", corresponding to identity proofing and verification.

The next deliverable from LEPS activity 7 is taking a deeper insight in costs and benefits for e-service provider, therefore providing more detailed analysis of what has been presented here as the main value proposition of LEPS project results: cost-effective connectivity to eIDAS eID services. The real challenges, however, remains long term sustainability, which can also be understood as cost-efficient connectivity. Unlike cost-effectiveness this analysis needs to look at operational issues, such as support or service level agreement, whether it is eIDAS node operator or identity broker (or whoever operates e-service connectivity to eIDAS eID services). In regard to these challenges, as well as other issues, the final deliverable D7.3 will present LEPS project recommendations, as well as feedback received from industry management group on the conclusions from the first phase of the project.

References

[1] ENISA, 2017, eIDAS: Overview on the implementation and uptake of Trust Services One year after the switch over, available at

https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services/at_download/fullReport

[2] eIDAS-NodeCountry overview, available at
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID

[3] eIDAS-Node Demo Tools Installation and Configuration Guide, available at
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+-+All+releases

[4] Federal Trade Commission report, March 2017, available at
https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

[5] Forrester study: Top Trends That Will Shape CIAM In 2018 And Beyond, available at
http://www1.janrain.com/rs/253-XLD-026/images/top-trends-that-will-shape-ciam-in-2018-and-beyond-industry-research.pdf

[6] Ponemon study, Global Trends in Identity Governance & Access Management, available at
https://www.ponemon.org/news-2/74

[7] Forbes, 2017 Is Quickly Becoming The Year Of The API Economy, available at

https://www.forbes.com/sites/louiscolumbus/2017/01/29/2017-is-quickly-becoming-the-year-of-the-api-economy

[8] Identity & Access Management Market - Global Forecast to 2021,
https://www.marketsandmarkets.com/PressReleases/identity-access-management-iam.asp

[9] UPU Measuring postal e-services development. A global perspective, available at
http://www.upu.int/uploads/tx_sbdownloader/studyPostalEservicesEn.pdf

[10] Marian Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith, On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards, available at:

https://saschafahl.de/papers/npa2013.pdf

[11] Australian Post White paper: A frictionless future for identity management, available at:

https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf

[12] Kjell Hansteen, Jon Ølnes and Tor Alvik, Nordic digital identification (eID): Survey and recommendations for cross border cooperation, 2016, available at

https://www.diva-portal.org/smash/get/diva2:902133/FULLTEXT01.pdf

[13] European Banking Authority Discussion Paper on strong customer authentication and secure communication, available at

https://ec.europa.eu/digital-single-market/en/blog/eidas-and-eba-discussion-paper-strong-authentication-0

[14] Observacion de administracion electronica, Boletin de febrero 2018 available at https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Boletines.html#.WthWXC5ubGg

[15] Eurobarometer, 2016, Financial Products and Services, available at:

https://data.europa.eu/euodp/data/dataset/S2108_85_1_446_ENG

[16] Accenture, 2013, The Future of Identity Banking, available at: https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_9/Accenture-Future-Identity-Banking.pdf

[17] Secure eID News, 2017, eIDAS digital ID finds use in cross-border European banking, available at: https://www.secureidnews.com/news-item/eidas-digital-id-finds-use-in-cross-border-european-banking/

[18] Consumer Financial Services Action Plan: Better products and more choice for European consumers, available at

http://europa.eu/rapid/press-release_IP-17-609_en.htm

[19] Digital Transformation in the Postal Industry, MIT Center for Digital Business, available at (password protected):

https://www.ipc.be/en/reports-library/publications/ipcreports_brochures/digital-transformation

[20] eGovernment Benchmark 2017, Final Insight Report Vol.1, A study prepared for the European Commission DG, available at

https://publications.europa.eu/en/publication-detail/-/publication/696b493e-f9a8-11e7-b8f5-01aa75ed71a1/language-en

[21] Study on the use of Electronic Identification (eID) for the European Citizens' Initiative, done by Everis on behalf of EC, September 2017, available at

ec.europa.eu/citizens-initiative/files/eID_ECI_Final_Report.pdf

[22] Cross-border e-commerce shopper survey 2017, IPC, available at

https://www.ipc.be/en/reports-library/publications/ipcreports_brochures/cross-border-e-commerce-shopper-survey-2017

[23] Post Office Network Business Development Group, Refresh - Renew – Reinvent , report from Irish Post Office December 2015, available at

https://www.chg.gov.ie/app/uploads/2017/02/post-office-report-english-january-2016-hr.pdf

[24] Riding the Waves of Postal Digital Innovation, USPS report , July 2016, available at

https://www.uspsoig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-014.pdf

[25] eIDAS Regulation: eID – Opportunities and Risks, Jens Bender, 2015, available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Bender.pdf;jsessionid=DBB620AC34096EE474854FB7E3DA2573.1_cid351?__blob=publicationFile&v=1

[26] Study on Cross-border Use of eID and Authentication Services to support student mobility and access to student services in Europe, available at https://ec.europa.eu/digital-single-market/en/news/study-cross-border-use-eid-and-authentication-services-support-student-mobility-and-access

[27] The world is going mad for mobile: Are government-sponsored ID implementations keeping up?, Joint whitepaper by Silicon trust and Infineon Technologies, available at www.infineon.com/mobileID

[28] Strategic thinking, article from Postal and Parcel technology magazine, available at http://www.postalandparceltechnologyinternational.com/articles.php?ArticleID=604

[29] Measuring postal e-services development, UPU Report, available at http://www.upu.int/uploads/tx_sbdownloader/studyPostalEservicesEn.pdf