WHITE PAPER

DIGITAL RESIDENCY PROGRAM PORTUGAL

PTER

DOWNLOAD PORTUGAL

STARTUP PORTUGAL

SEPTEMBER 2020

CONTENTS

DOWNLOAD
PORTUGAL

OVERVIEW

This report outlines a proposed strategy for Portugal to develop a world-leading Portuguese e-residency program (PTER), building on the initial work carried out by AMA and Startup Portugal. The report is intended to add additional input to support the work being carried out by AMA to develop e-residency for Portugal.

The report is written by Patrick Curry, an international expert in identity, and Tobias Stone, a former Special Advisor to Estonia's e-Residency program. They have formed an e-residency advisory team engaged by Startup Portugal to share their experience and insights relating to e-residency, and to international identity activities. The aim of this report is to support the activities of the Portuguese Government, and in particular of AMA and Startup Portugal to enable Portugal's e-residency program to become world leading.

The intention is for PTER to start by offering foreign freelancers and startups a digital company based in Portugal, and then quickly develop it to support existing foreign companies doing trade in Europe, and with the rest of the world. These companies seek a high assurance, high value identity system that can support international trade, positioning Portugal as a trading gateway to Europe, and PTER as an internationally recognised digital identity that can be used for a wide range of business activities. This will attract tax revenues from companies locating in Portugal to do business in Europe, and fees, for example from Relying Parties, such as banks, that could use PTER to carry out KYC and AML checks, and much more.

The report builds on the work done by Startup Portugal and AMA, adding details to the complexity of developing a high assurance identity, and explains how this can be used for interactions between individuals and the government, and also individuals and industry. It is the industry use-case that will make this program valuable and will lead to people using it as part of their daily lives.

A few other countries have tried this, but they failed to realise the full potential because they did not take e-residency beyond being a tool for freelancers and startups, and they were not compliant with global standards to ensure interoperability, or with regulations such as GDPR, PSD2, AML for data protection and anti-money laundering. If Portugal takes PTER to this next level, where the demand really lies, it has the potential to be used widely by banks, regulated industries and governments. Today, Portugal has first mover advantage as it has no competition; done well, PTER could quickly become an identity asset recognised by countries around the world.

If Portugal's e-Residency is developed as a high-assurance identity operating within international standards, it could position Portugal as the base for foreign businesses operating in Europe, and for European businesses operating outside Europe.

This document outlines our understanding of what AMA has already done and is planning to do, and supplements this with further actions and considerations. These are intended to build out PTER beyond individual-to-government interactions, and beyond startups and freelancers, to become a valuable service for corporations, and for Relying Parties, such as banks and other government agencies.

We also examine how to develop governance for the program, and ensure it complies with rapidly evolving international standards in order for it to reach its full potential.

TEAM BACKGROUND

Patrick Curry OBE CEng MIET MBCS

Global expert in identity, security, and federated information sharing. Patrick is currently working with leading companies, UN, WEF, ISO and various government departments to extend the national implementation of federated trust, secure collaboration, distributed decision-making and the sharing of high quality data under control. He has 25 years' experience in transatlantic and European secure collaboration and the sharing of sensitive information including cybersecurity and counter-fraud. To enable this, there has been a huge effort on identity management and federated trust. Previously he was the main facilitator between the US DoD and aerospace industry on the alignment of part marking standards and Unique Identification of tangible assets to enable Total Asset Visibility. Previous military career in command, operational planning, procurement, information management, IT management, logistics and counter-terrorism. He was awarded the OBE by HM The Queen, and has two UK and one US industry awards.

Dr Tobias Stone BA (Hons) MSt (Oxon) PhD

Former Special Advisor to the Head of e-Residency, Government of Estonia, and former policy advisor to the UK government's Cabinet Office on support of the startup sector, and sits on the Smart London Board advising the Mayor of London on tech sector strategy. Tech entrepreneur, investor, and professional board director, with extensive international and cross-border business experience. PhD in business sociology and innovation, and honorary practice fellow at Imperial College Business School.

01. DEFINITIONS

Identity, identification, and authentication are some of the many important terms in broad topic of digital identity, trust management, and identity federation. Having clear definitions ensures precision and clarity in the development of the necessary policies, procedures and mechanisms. Here are some important definitions of terms used in this document:

Authentication

The provision of assurance in the identity of an entity. [ISO/IEC 18014-2]

Authentication factor

A piece of information and/or process used to authenticate or verify the identity of an entity. [ISO/IEC 19790]. NOTE: Authentication factors are divided into four categories:

- something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
- something an entity knows (e.g., password, PIN);
- something an entity is (e.g., biometric characteristic); or
- something an entity typically does (e.g., behaviour pattern).

Authoritative source

A repository which is recognised as being an accurate and up-to-date source of information. [ISO/IEC 29115]. Only an authoritative source is considered legally admissible. An example would be the Passport Office that is the authoritative source for passport numbers.

Credential

A set of data presented as evidence of a claimed or asserted identity and/or entitlements. [ISO/IEC 29115]

Identifier

One or more attributes that uniquely characterize an entity in a specific context. [ISO/IEC 29115]

Identity

A set of attributes related to an entity. [ISO/IEC 29115]

Identity proofing

The process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance. [ISO/IEC 29115]

Non-repudiation

The ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action. [ITU-T X.1252]

Relying Party

An actor that relies on an identity assertion or claim. [ISO/IEC 29115]

02. INITIAL UNDERSTANDING

Government leaders have tasked AMA to begin developing Portuguese e-residency and asked Startup Portugal to provide the business leadership, input, and engagement so that it quickly becomes successful.

Success depends on effective collaboration, a strong business case, and extensive international experience. With these, PTER can grow its user community and the market for PTER-based services.

Digital identity and identification, and their links to the physical world, are a complex subject. As new digital technologies emerge and more governments impose more regulations, so digital identification is becoming more complex.

This report deliberately avoids complexity, but the authors can go deeper as stakeholders require and PTER progresses.

03. KEY FINDINGS

Some key findings identified so far, which will be addressed later:

1. There is no business requirement for two tiers of e-residency because **only a High Assurance identity will be of value to regulated industries**, therefore we will focus on achieving the High Assurance tier immediately. See Appendix 2 - Determining Levels of Assurance and Levels of Identity Proofing - for a more detailed understanding and justification for High Assurance.

2. It will not be necessary to use embassies and consulates to create a higher level of identity. Using embassies and consulates increases risks, costs, and delay. **We believe we can produce a High Assurance online-only identity from the outset** for most countries, although a few high-risk countries may require additional countermeasures.

3. PTER should use EU-certified High Assurance online remote enrolment in accordance with international standards

4. PTER must meet international standards and be regulatory compliant before industry and consumers can use PTER. We will outline a series of user-to-industry use cases to supplement the AMA list, which is primarily user-to-government

5. PTER should be **based on validation of real-time passport data from authoritative sources, supported by corroborative data from other sources and real-time monitoring**. This will allow it to be High Assurance and therefore of greater value to the government and to industry

6. **We do not think eIDAS alone is suitable for creating a PTER identity**. eIDAS is designed for government-to-citizen (G2C) interactions, and is not be suitable for many business-to-consumer (B2C) uses, nor is its liability model commercially acceptable

7. We do suggest notifying PTER under eIDAS, so it would have to be accepted by public authorities throughout Europe by EU law. **This would make PTER the e-ID of choice for none-EU persons and organisations**, as well as EU citizens that do not have a suitable eIDAS credential.

8. We anticipate that Portugal will work with approved private sector identity providers (IDP) to leverage what these companies have already spent years and millions of Euros building. As more IDPs use PTER, so the market will grow.

9. **This will enable PTER to carry out additional checks when an individual's PTER identity is created, and will enable PTER to ensure that the identification of foreign nationals is validated regularly to remain up to date.**

10. There are multiple ways in which PTER can create financial and public benefit for Portugal. Some of these are outlined below, and range from taxation through to service fees.

04. FUNDAMENTAL PRINCIPLES

The following points form the fundamental principles that will define how PTER is designed and rolled out.

- PTER is about foreign persons not about Portuguese citizens.
- PTER is for people wanting to do business in Portugal and also through Portugal in other countries, particularly in the EU.
- To do this, PTER users need to have a Portuguese company, a Euro bank account, and the ability to interact with Portuguese government organisations digitally.
- PTER will have a standards-compliant, best-practice risk-mitigation strategy that covers all participating stakeholders and their shared risks. This will include a liability model covering key business risks, some of which should be covered by insurance.
- PTER enables significant opportunities not only in Portugal's digital economy and society, but also potentially **provides a digital gateway for cross-border business and physical trade into and across the EU, including from the USA.**
- PTER has the potential to do the same in reverse and **provide the ability for EU citizens to do business in non-EU countries, such as the USA or South America**, using PTER to identify themselves and carry out transactions.
- PTER provides Portugal with the ability to exploit new digital technologies, including AI and Blockchain, particularly across the EU, working with the European Blockchain Partnership of governments created by the European Commission.
- PTER involves remote enrolment at High Assurance. It does not use embassies, which add costs, delay, and risks. However, embassies could offer new services in the future, based on PTER.
- PTER will use secure mobile phones from the beginning. It should integrate with Web for secure laptops in the near future. **There is no plan for a card, which adds costs and risks.**
- PTER also anchors to the devices bound to the identity to support Multi-Factor Authentication (MFA) and to defeat SIM swap attacks.
- PTER supports **digital signatures, encryption, and email signing** (for secure email).
- PTER could potentially support logical access control (LACS) at the application or the network level.
- It may become possible in the future for **PTER to support Physical Access Control** (PACS) for building access, visitor access, flight boarding, border control and similar requirements.
- PTER anchors to passport data and some national e-IDs for many reasons, including legal, and **includes real time monitoring**. However, it also checks many other factors in the background and uses high assurance biometric processes certified by the EU and ISO. It can also leverage other documents and digital credentials, including eIDAS.

- PTER cannot rely solely on eIDAS to create a PTER, for legal, fraud and liability reasons. However, PTER will be able to exploit eIDAS replacement capabilities including EBSI[1] and ESSIF[2].
- PTER could be notified under the eIDAS scheme to become legally acceptable by governments throughout the EU.
- PTER should synergise with Portugal's three pre-notified eID schemes: the national eID card (Cartão de Cidadão - CC), the mobile eID solution (Chave Móvel Digital - CMD) and the Professional Attributes Certification System (Sistema de Certificação de Atributos Profissionais - SCAP).
- **PTER will require an appropriate governance model that includes all the major stakeholder groupings that use, rely upon, assure, insure, control and provide services for PTER.** This model will include industry stakeholders, both within and outside of Portugal. To be credible, it must be neutral and transparent, and based on best practices. **We anticipate a foundation or 4th sector organisation being established to manage the governance**; suitable models already exist.
- PTER will require the assistance and collaboration of several Portuguese government departments, agencies, law enforcement, cybersecurity, and regulators.

[1] European Blockchain Services Infrastructure.
[2] European Blockchain Self Sovereign Identity Framework

05. LESSONS FROM ESTONIA

Estonia created its e-Residency programme to offer non-residents access to a some of the country's online services. It used many of the features of the Estonian citizen e-ID, which is issued to citizens and residents, and enabled non-residents to form a company, submit tax returns, and notarise documents.

Since the launch of the program, the number of e-residents has grown to surpass 62,000 (Nov 2019), and e-residents have established over 10,100 companies in Estonia that employ some 1,700 people in total.

The original interest behind e-Residency was to increase GDP by increasing the number of people working and paying tax in Estonia without requiring people to move there. This then evolved, and the focus shifted to e-Residents establishing companies in Estonia to do business there and in Europe. The financial benefits to Estonia are a mixture of tax paid by these companies, and the associated economic benefit they create by hiring local professional service companies to do accounting, and other activities.

A significant indirect benefit of e-Residency has been to promote Estonia around the world as a leading digital nation, and to encourage e-Residents to visit Estonia as tourists. The associated PR benefit has been hard to evaluate, but is a clear benefit of the program.

Early limitations of e-Residency were that people applied for e-Residency out of curiosity, but never used it. More recently the program has tried to focus on freelancers and startups who establish companies and use them to do business. The other limitation of e-Residency was considerable difficulty faced by the program in finding banks to open accounts for e-Resident companies.

The program was launched as a 'government startup' with a small budget and team. This was seen as very forward thinking by Estonia, but limited its ability to grow in the early days.

It is a misunderstanding to think that e-Residency was a technology project. E-Residency was primarily a policy initiative, requiring the government to change laws rapidly to create a legal environment in which, for example, a non-resident could open a company online from abroad, and later that a bank account could be opened over video call, rather than in person. The associated technology was not commissioned centrally by the government. Each ministry was able to commission its own solutions as needed.

5.1 Positive lessons

- For historic reasons, the Estonian government has a very strong digital awareness and has developed a highly integrated and coherent digital infrastructure to provide a single way for citizens and businesses to interact with government. E-Residency leverages this.
- E-Residency has been strongly and directly supported by the President, Prime Minister, and the Cabinet from the beginning, and the programme manager and his supporters had direct access to the Prime Minister, President, and relevant leaders across government. In particular, it was directly championed by the country's CIO, and the Head of Digital Government.
- Estonia has enjoyed first-mover advantage, and it is consequently well known around the world.

- E-Residency promoted the ability to create a company quickly and easily online, and also to open a euro bank account.

5.2 Learnings

- E-Residency is based on police passport checking and recording of a fingerprint at an Estonian embassy, both of which are isolated, weak processes. They do not provide live or ongoing checks of the user's identity.
- The Estonian Police & Border Agency is responsible for these checks but would not disclose the identity proofing policies or procedures behind these checks, so relying party organisations, including other governments, have been cautious about accepting Estonia's e-Residency in a variety of situations.
- We believe there is no monitoring of passports or data validation against the issuing authorities. This means that if a passport that has been used to establish an e-Residency is later stolen, revoked, renewed or changed, e-Residency is unaware until notified.
- The initial business case was targeted at individuals and micro businesses. There was no plan for engagement with larger businesses, which missed a significant opportunity.
- There has been no significant attempt to assist Relying Parties to provide new services. (Compare this with FEDICT IBZ, which enabled the creation of over 500 applications using the Belgian e-ID). Relying Parties (see below) are banks and other authorities that need to check a reliable identity. Offering to support new services could lead to revenue for the country.
- E-Residency has not created a market with Identity Providers and Relying Parties.
- The programme ran into difficulties with banks. Proper KYC/AML[3] arrangements were not made with the Estonian banks. A Latvian bank began to support E-Residency but a regulatory audit identified failures, so the bank went into regulatory "special measures" during an investigation, and the use of Estonian E-Residency was paused. This damaged the E-Residency brand.
- E-Residency was not clear how it would be used when it was launched. It has taken time to understand what it is for. Portugal can benefit from those lessons, and launch a program with a clear business and market strategy from the outset.

[3] Know Your Customer (KYC), Anti-Money Laundering (AML).

06. OTHER COUNTRIES WORKING ON E-RESIDENCY PROGRAMS

No country has yet followed the Estonian e-Residency model, although Netherlands and Singapore have thought about it, and Lithuania announced it would launch a similar program. Other countries have made enquiries about 'buying' e-Residency, but as explained it relies primarily on a complex coordinated development of government policy, rather than on a piece of technology that can be purchased or built.

- **The Netherlands** understand the potential and are discussing possibilities but, as far as we know, there is no formal plan to proceed. The NL is one of the most collaborative and innovative digital nations in Europe, where many international businesses are based, so e-Residency would find a ready market.

- For tax reasons, several global companies have their European/EMEA headquarters in Dublin with large workforces who could benefit from e-residency, particularly as foreigners move in and out of the country. Ireland has no national e-ID and no plans to introduce one. Industry initiatives are being discussed but they don't include e-residency.

- **Malta** is the second biggest gaming/gambling centre in the world (over 250 companies) and has a large financial services sector. Its attempts at e-ID have focused on electronic voting, not on government services or business. E-residency has been discussed at ministerial level, but there has been no action yet. The international and EU KYC/AML requirements for gaming are significant. They have a very strong need for e-residency to satisfy Maltese and EU regulations. Some work has been done by the gaming companies that an e-residency could support today.

- **Singapore** is moving to a digital and mobile eID, MyPass for people and ComPass for companies. They have a foreign worker ID card which will become digital soon. Many foreigners visit Singapore to do business. The situation is ideal for an e-residency and there is some interest in developing e-residency when the current initiatives are fully deployed.

It is the nature of e-residency that if these countries do not have e-residency, they may want to use the e-residency of another country. **If PTER is developed into a very sophisticated high-assurance identity that operates within international standards, it could be adopted by other countries to solve some of their requirements. Estonia has enjoyed first-mover advantage, and it is consequently well known around the world.**

DIGITAL CITIZEN PERKS

DOWNLOAD
PORTUGAL

PTER

JUMPSTA
BUSINESS
IN EUROPE

JOIN PORTUGAL'S E-RESIDENCY PROGRAM

STARTUP PORTUGAL

07. KEY POINTS FOR SUCCESS

Most national identity schemes in democracies fail to deliver benefit when they are only for citizen to government use. Key lessons:

7.1 To succeed, PTER needs to be used frequently

Successful schemes require regular, even daily, use by the user otherwise the user forgets how to use it and the scheme does not achieve wide adoption

If PTER only enables users to carry out transactions that are infrequent, for example an annual tax return, then people never get into the habit of using it. They will forget passwords and not learn the various processes. PTER needs to be relevant to regular activities, and be a better experience than doing these things conventionally. That will encourage people to use it frequently, so it becomes a regular part of their daily business life.

This means PTER needs to work between individuals and companies, and between companies, as well as offering the individual ways of engaging with the government. PTER needs to have value for transactions between:

- Individual → Portuguese government
- Individual → Other governments
- Individual → Portuguese Company
- Individual → Portuguese Individual
- Individual → Foreign Company
- Individual → Foreign Individual
- Company → Company

PTER users could be natural persons or legal persons.

7.2 Over 95% of authenticated user transactions are for non-government purposes

In general, over 95% of authenticated user transactions are for business or consumer purposes because there are many more business and consumer use-cases than there are between users and government. As it will be essential to encourage daily or frequent use of PTER, it is important that it is useful for business transactions, and not just transactions with government. For example, people submit a tax return annually, but sign documents or use their bank frequently.

7.3 Example use cases include:

Government transactions

- Register a company
- Obtain a business licence to operate (e.g. to sell prescription drugs)
- Submit a tax return
- Register a business vehicle
- Register ownership of a building
- Register rental or occupation of a building
- Register as a government contractor
- Bid for government contracts
- Conduct contract business with government organisations
- Report incidents to police
- Support multichannel/omnichannel models (iSimplex)

Business transactions

- Open a bank account in Portugal
- Recruit staff in Portugal and abroad
- Sign a contract with a Portuguese entity
- Sign a contract with a regulated Portuguese entity
- Sign a contract with a European entity
- Open a bank account in Europe
- Open a bank account outside Europe / in USA
- Manage user consent and privacy
- Send and receive signed and encrypted mails
- Send and receive secure payments
- Comply with AML and KYC financial regulations
- Invest in a Portuguese or EU company
- Make compliant secure cross-border payments
- Access health records
- Authenticate for requesting Covid-19 tests and to receive test results
- Obtain and manage a Covid passport
- Notarise a document
- Deliver controlled goods and drugs securely to the correct person
- Buy a phone or a SIM card
- Book a flight and check in with an automated passport validation
- Book a hotel and check in with an automated passport validation
- Book a car hire and collect it with an automated driving licence validation
- Participate in online training courses
- Sit academic and professional examinations online

7.4 The role of government in supporting PTER

Government has three significant roles:

- Give confidence to government and industry organisations and users, and to consumers that PTER will quickly grow from small beginnings and that it will be benefits-led, not government-driven, for the public good. This requires top level leadership and backing with adequate resources. The lesson from Estonia here is clear, where the President and Prime Minister were vocal advocates of the program.
- Establish a collaborative governance model that addresses shared risks and enables all stakeholders to engage together. Every organisation should be both a customer and supplier.
- Provide a non-executive coordination & expert focus within government to help individual government organisations leverage PTER for Portugal's digital economy and society.

7.5 PTER is for foreigners

PTER will need to meet the requirements of foreign companies in order to become truly valuable, otherwise foreigners will only be able to use it to do business within Portugal. **PTER can then help foreign companies operating in Portugal and also doing business in the EU from Portugal, which is where the real value lies.** The same could happen in reverse, helping businesses in other parts of the EU do business outside the EU, via Portugal.

If PTER is developed as a high-assurance identity operating within international standards, it could position Portugal as the base for foreign businesses operating in Europe, and for European businesses operating outside Europe.

PTER should also be for foreigners who have or work for companies in Portugal and are visiting Portugal. This means it could provide services related to employment and local travel.

7.6 Benefit to Portuguese citizens

PTER needs to benefit Portuguese citizens by bringing business to the country, and creating new business opportunities for them. It may also become useful as a bridge between Portugal and other jurisdictions. It is essential that PTER only offers foreigners benefits already available to Portuguese citizens and residents. Any instance where PTER offers more benefits to foreigners would need to be addressed to ensure that benefit is available to Portuguese residents as well.

08. USER ORGANISATIONS

In 2017, the EU-28 business economy was made up of 27.5 million active companies with more than 150 million employees. Today, there are more. Many types of business organisations in each industry sector across the EU classification list will be interested in PTER:

A	Agriculture, Forestry and Fishing
B	Mining and Quarrying
C	Manufacturing
D	Electricity, Gas, Steam and Air Conditioning Supply
E	Water Supply; Sewerage, Waste Management and Remediation Activities
F	Construction
G	Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles
H	Transportation and Storage
I	Accommodation and Food Service Activities
J	Information and Communication
K	Financial and Insurance Activities
L	Real Estate Activities
M	Professional, Scientific and Technical Activities
N	Administrative and Support Service Activities
O	Public Administration and Defence; Compulsory Social Security
P	Education
Q	Human Health and Social Work Activities
R	Arts, Entertainment and Recreation
S	Other Service Activities
T	Activities of Households as Employers; Undifferentiated Goods and Services Producing Activities of Households for Own Use
U	Activities of Extraterritorial Organisations and Bodies

However, there are three major areas common across most of these industry (and government) organisations, all of which have increasing requirements for KYC, AML and authentication:

- **Money:** Payments, trade finance, taxes and customs tariffs;
- **Asset tracking:** the movement of goods, vehicles and people;
- **High quality data:** shared data to support all digital business and regulatory activities.

If PTER is to become an international success, it needs to address these three common activities in a sophisticated and internationally recognised way. This would increase its value to larger corporations and other governments, as well as freelancers and startups.

09. MARKET ANALYSIS

PTER will be launched by the government with business cooperation and will be scaled by business. As the majority of transactions are for business activities, it will be possible to identify the companies, government organisations, industry sectors and activities that cause PTER to spread virally. An Estonian example of this is when foreign investors invest into an Estonian company they are asked to apply for an Estonian e-Residency in order to be able to sign shareholder resolutions and other contracts, all of which are managed digitally. This grows the user base in an influential business sector organically.

As PTER is described in this document, it would have no competition in this e-residency market at the moment. **PTER has first-mover advantage, but it will have to move quickly to maintain that advantage.** This will require a high degree of coordination and cooperation, which Start Up Portugal is well positioned to provide.

Early engagement with market makers or "anchor stores" as they are known in the USA, will help considerably. These are major or global companies in each sector who dominate supply chains; once they are on board, their entire supply chain and customer base is likely to follow suit. The Advisory Team has extensive experience of leveraging anchor store organisations, in governments and industries, to magnify the attractiveness of PTER, and there are ways in which such anchor stores can be incentivised to participate. Once that happens, having and using PTER is just a cost of doing business. It becomes the New Normal.

10. FUNCTIONALITY AND TECHNOLOGY

If Portugal can build an e-Residency that combines a high assurance digital identity with international standards, then **significant benefits flow from capabilities that would be enabled by PTER**. These are:

1. Strong digital signatures
2. Support for technical non-repudiation (see definitions).
3. Strong authentication
4. Strong encryption
5. Trusted interoperability between disparate systems
6. Synergy with national and international identity management initiatives
7. Multi-factor authentication (see definitions)
8. Network security
    a. Access control
    b. Secure tunnelling
    c. Single Sign On
9. Federated trust, where multiple identity authorities operate under an agreed single Common Policy to enable parties to trust each other across the federation.

Various technological options are available to PTER, however today the move is away from a classic, early-bind, evidence of identity, credential issuing model, which tends to result in data proliferation, loss of user control and significant operating costs. Instead, the move is towards **real-time data validation against authoritative data sources**, where a user has a secure application and they are strongly bound to their phone and to the SIM in the phone as the result of a high assurance identity proofing & enrolment process.

This data-centric, mobile-centric approach avoids many of the issues, complexities and costs of making different technologies and protocols interoperate, as well as avoiding data centralisation. It also:

- Makes federation easier, which is essential for cross-border operations and for a market approach;
- Gives users more control over personal data and the data controller more confidence that the user is the person who "owns" the data;
- Increases privacy, particularly with regard to GDPR, the e-Evidence Directive, and the e-Privacy Directive;

- Enables authoritative data sources to update Relying Parties directly when there is a legal requirement to do so, without needing user consent;
- Supports legal requirements for policy enforcement and for law enforcement investigations authorised by a court of law;
- Enables the binding of additional attributes to meet different regulated industry requirements;
- Provides greater resilience and therefore greater availability.

11. HOW PTER CREATES REVENUE FOR PORTUGAL

To succeed, PTER needs to encourage the creation of a market that depends on PTER. There are two market drivers for this market:

1. Government regulation

The Portuguese government mandates the use of PTER for foreign access to its digital services, which reduces costs and risks, and provides revenue and taxes from foreigners creating new companies.

2. Business benefit

- Businesses benefit from providing services to a growing market of customers in Portugal, inside the EU, and outside the EU.
- **Businesses will be able to meet requirements more easily, such as KYC, and the savings they make will justify paying for this service.**
- PTER will be vital to help these businesses provide trusted services that are faster, better, and cheaper.

11.1 Benefits to the Portuguese Government

1. Increasing foreign investment and economic activity in Portugal;
2. Increasing the economic benefit to Portugal by offering digital trust services that work across Europe and beyond.
3. Increasing international, remote access to the single European Market, in support of digital services as well as supporting the movement of physical assets in supply chains and payments. Portugal could, in time, become a digital gateway to Europe, similar to Rotterdam for maritime trade.
4. Increased tax revenue from these activities when they are carried out through Portuguese companies.

11.2 How the community of users around PTER can generate revenue for the government

Although the Portuguese government may pay for PTER services, it is the Relying Parties that will drive the money flow for PTER activity. These are primarily businesses, like banks, who rely on authoritative data sources (such as Portuguese issued digital identities) in order to comply with international standards, such as KYC and AML. **This very significant market could become a source of revenue for the Portuguese government, as well as a key driver for people to use PTER.** This community of users consists of different parties who need to interact with each other:

1. End customers for a service: persons and companies; natural persons and legal persons.
2. Relying Parties (RPs): companies and government organisations that provide those services, for which we believe they will pay PTER to enable the customer to authenticate, sign, prove KYC compliance and more. **This could become a significant potential revenue source for the Portuguese government.**
3. Authoritative data sources: these organisations are authoritative sources for specific data, defined in law or by contractual agreement. An example is a national passport office.
4. Trust service providers (TSPs). These provide the technologies and services to enable PTER, the authoritative sources, and the RPs to work within the overall PTER trust framework.
5. PTER's organisation. PTER's governance regime will need to onboard RPs and authoritative data sources either directly or via TSPs.

Together this community will generate interactions that either save or make money, which is where Portugal can charge fees to use PTER.

11.3 Example Revenue Sources

Some examples of how PTER could create direct and indirect revenues for the Portuguese economy include:

Startups and freelancers

The simplest versions of PTER is a foreign startup or freelancer who wants a company in Europe. They may be using this to contract and invoice clients elsewhere in Europe. These people may be from outside Europe, or may be from countries with more complicated and expensive company formation processes. These users will generate revenue for Portugal by employing local service providers (accountants, service agents), and potentially by paying corporation tax.

A lateral advantage of PTER will be that it promotes Portugal, and will encourage people to come to Portugal. This was the case with Estonia, where e-residents developed an affinity with the country, and this encouraged them to visit, or even to move there.

KYC and AML for Relying Parties

A big requirement is Know Your Customer (KYC) compliance with the EU 5th Anti Money Laundering (AML) Directive and Payment Service Directive 2 (PSD2), as well as other legislation. PSD2 requires Strong Customer Authentication (SCA) for online payments above €30, and for Open Banking. AML5 requires KYC checks for commercial payments above €10,000. If built correctly, PTER could support this in real time, significantly reducing the costs incurred by Relying Parties such as banks, and will enable them to do it in a much more privacy-friendly way, reducing GDPR risks and costs.

As an example, KYC validation for new bank account opening in London alone is worth more than €200M a year. Existing paper legacy systems cost many, many times that and are less effective. Banks are constantly searching for a more efficient way to do this. We believe we could develop PTER to become an attractive solution for non-Portuguese banks to carry out KYC on new customers, creating a cost-saving that can partly be passed on to the Portuguese government.

DIGITAL CITIZEN PERKS

MANAGE YOUR TAXES FROM YOUR PHONE

PTER

DOWNLOAD PORTUGAL

JOIN PORTUGAL'S E-RESIDENCY PROGRAM

STARTUPGAL

12. RECIPROCITY AND MUTUAL RECOGNITION

Reciprocity and mutual recognition refers to other countries recognising the Portuguese e-residency as a high assurance form of identity that operates within international frameworks. If PTER can be recognised in this way, this principle of reciprocity opens up additional opportunities.

There are at least three areas where this could be considered:

1. A PTER user within the EU being able to do business across the EU
2. A PTER user outside the EU being able to do business across the EU
3. A PTER user within the EU being able to do business outside the EU in specific nations

12.1 International trade into Europe

Another significant requirement is to enable "frictionless trade" and reduce the costs and fraud in trade finance, particularly across borders. This also has to be linked with product traceability and end to end tariff code transparency for regulators and tax authorities. Rotterdam is the largest EU port and it handles more than 90% of the EU's international maritime trade – it is the gateway to Europe. Companies all along the supply chains would welcome a common means to authenticate employees, which PTER could help make happen. **If companies using Rotterdam could use PTER as the underlying digital identity to manage employees and customs, based from companies in Portugal, this would be a very significant win for Portugal.**

Overlapping with this is the need of businesses in the USA and other non-EU countries that seek to do business in the EU. **One early win could be to provide company officials of companies registered in Delaware with PTER credentials so they could do business in the EU.** Not only could this meet EU regulatory requirements, but this could also meet US regulatory requirements that currently limit US citizens' ability to own property outside the USA. **This could make PTER, and Portugal, the single access point to the EU's digital economy from Delaware.** (Note that Delaware has the biggest company register in the USA, partly due to its favourable tax policies).

12.2 eIDAS

eIDAS is described in the next section. It does not meet the needs of industry. PTER can exploit this situation in two ways:

- Use an eIDAS credential, where it is available, as an additional authentication factor in a chain of trust, to strengthen the identity proofing and/or authentication underpinning PTER;
- PTER could be "notified" (see below) under eIDAS, which would increase the business cases where PTER could be used.

12.3 Becoming a European ID that can be used for transactions in the USA

Many EU businesses seek ways in which they can do digital business more effectively in the USA and many other non-EU nations, in just the same way that they would do in the EU. There are several ways in which PTER could potentially be recognised either nationally or at state level in the USA. The need for better identity in the USA is strong for many reasons. Government initiatives are mostly at state level but with some coordination at a national level. There is no equivalent of PTER in the USA, which could address this need for foreigners.

This situation creates a window of opportunity for PTER in the USA and other countries outside the EU.

12.4 Becoming a European ID that non-Europeans can use globally

Extending the model, there are further use cases, such as an American seeking to create a company and open a bank account in the UK by using PTER.

12.5 Enabling Portuguese-owned companies to benefit

If, in the future, PTER is able to support the above use cases, then it should be possible for Portuguese citizens who are abroad to have similar access to PTER capabilities, such as Portuguese citizen owned businesses being able to do business in the USA by forming a company in Delaware.

13. LEVERAGING INTERNATIONAL INITIATIVES

Many emerging international initiatives require some form of re-usable high assurance identification and authentication. Four areas stand out at the moment, all of which could benefit from PTER:

- **Finance –** KYC/AML, PSD 2 and SCA (already mentioned), cross-border payments, Covid-19 business payments;
- **Travel and movement –** online bookings, check-in, airport screening, border controls. See KTDI below.
- **Health –** Covid-19 antigen and antibody testing. There are several initiatives.
    - Demand for effective test kits is rocketing. Providers and authorities are increasingly concerned about how the test kit ordering & delivery, the testing and the results can be securely managed and bound to the correct person throughout.
    - Covid passports are being developed for various purposes and with different results. Mainly, they are either to help provide a testing history for a person or employee or an exposure history for a person or employee. In UK, they are also being developed for clinicians to record their exposure to Covid-19 and also their experience at treating Covid-19.
- **Education and professional qualifications.** The rise in fraudulent claims of educational and professional qualifications is resulting in some governments, particularly in Europe, establishing registers that can be queried by relying party organisations. However, this is particularly difficult for foreign students and staff, and qualifications from foreign universities.

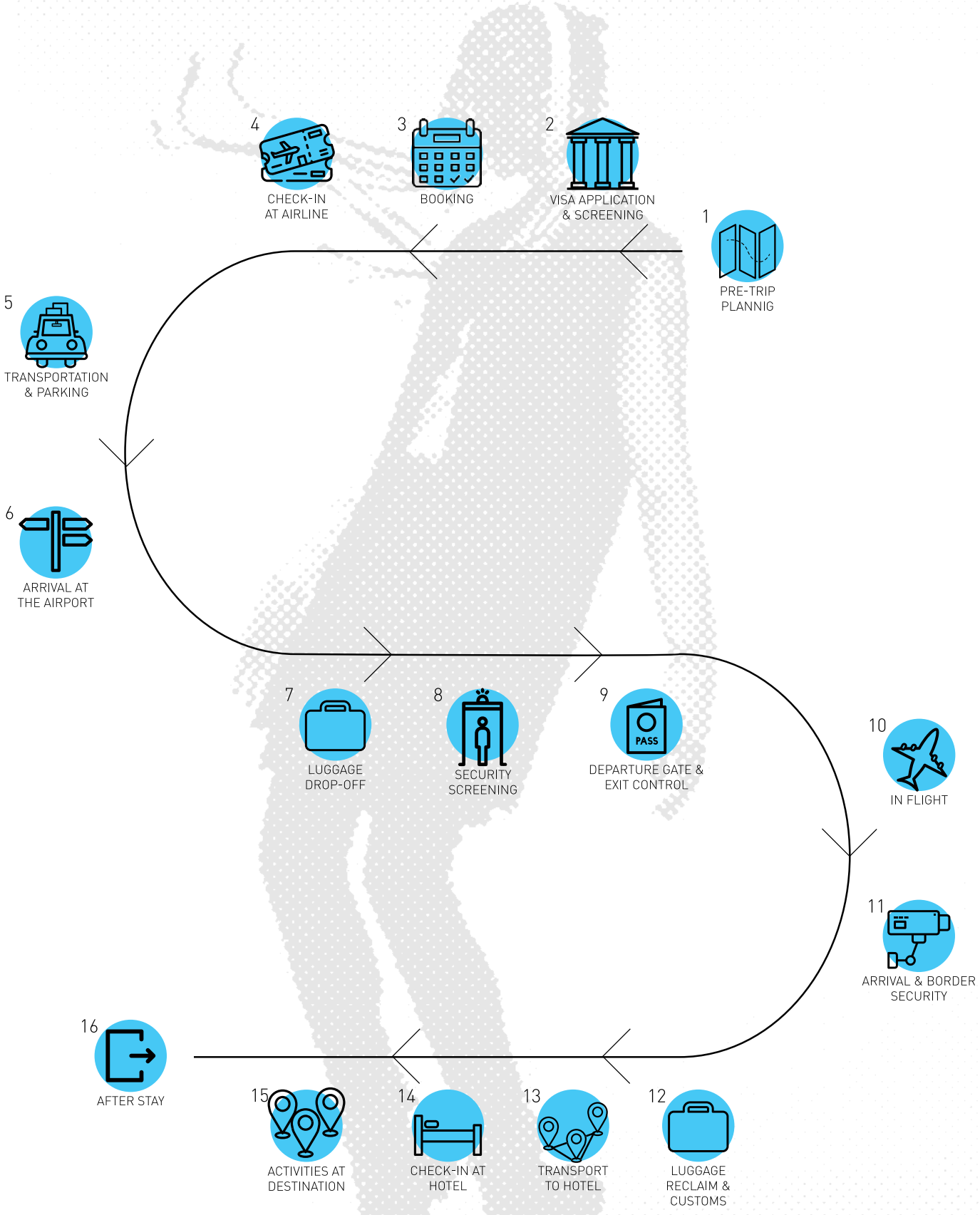
13.1 World Economic Forum Known Traveller Digital identity (KTDI)

KTDI is described as an international travel security initiative and it has links with the Mobile Passport initiative in ICAO and ISO, and IATA's One Identity. **KTDI seeks to provide a single digital trust model to support a traveller's journey based on authentication and data validation not on outdated documents.** In the past this was all geared around documents and checking them manually against the person, with unacceptably poor results. Now it is about using accurate data in real time with multiple touch points in the traveller's journey, starting with the ordering processes.

The figure below is from the WEF KTDI Concept Paper (publicly available). It illustrates the many touch points in a traveller's journey. **As PTER anchors to a passport and real-time passport data validation, and it is based on secure mobile, so it could potentially be one KTDI solution for most of these touch points.**

While Portugal is not currently involved in this project, PTER could help it work. **The KTDI partner companies and some governments already involved would be interested in PTER.**

13. LEVERAGING INTERNATIONAL INITIATIVES



14. THE EU PERSPECTIVE

14.1 Portugal's 2021 EU Presidency

The Presidency Trio of Germany, Portugal, and Slovenia has the potential to make a major contribution and promote concrete steps to drive a transformative agenda during the coming eighteen-month period. The core task of the German EU Council Presidency for the rest of 2020 is "to make mobility in Europe more modern, more innovative and more sustainable – and learn our lessons from COVID-19.[4]" The German Presidency's "New Mobility Approach" will be its response to the European Commission's "Green Deal". This means it intends to pursue a single approach comprising thee pillars: climate change mitigation, mobility, and digital transformation.

The Portuguese President has already announced that relations with India will be at the heart of the Portuguese Presidency, and the draft programme for the Trio announces that "an EU-India Leaders' Meeting is scheduled to take place in Porto in May 2021 at the invitation of the President of the European Council and hosted by the Portuguese Presidency". **This is a major opportunity to launch PTER as a Portuguese Presidential contribution to the Presidency Trio objectives, with an early emphasis to support EU – India economic and societal collaboration.** This will show that Portugal is the gateway for Indian companies to do business in the EU and potentially vice-versa.

If possible, a dialogue or an agreement could be reached before May 21 for the Indian government to agree to accept PTER credentials for an initial pilot. This pilot could be announced at the Leader's Meeting. This Advisory Team has links with relevant Indian government organisations and can assist in making this happen.

14.2 eIDAS

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market is known as eIDAS (electronic ID Authentication and Signature). If a nation "notifies" an identity scheme under eIDAS, then the notified scheme's credentials must be accepted by other member states for public purposes under a liability model between member states.

However, **the reality is that few nations have notified schemes to the Commission, and that little has been done to help the citizen use their eIDAS credential, if they have one, in another member state.** If a citizen presents an eIDAS credential to a public organisation in another member state, it is highly unlikely that the organisation will know what to do, and the experience is different in each member state.

For some time, the European Commission has been working to align the eIDAS quality specifications with Levels of Assurance in international standards so that eIDAS credentials could be more interoperable and attractive to industry, and also to find ways to address the liability challenges. However, there has not been adequate progress, mainly because governments have been focused on achieving adequate adoption and value with their own identity schemes, and are not yet in a position to accept cross-border schemes.

[4] https://www.bmvi.de/EN/The-Ministry/Germany-EU-Council-Presidency/germany-eu-council-presidency.html

The opportunity exists for a nation to notify a high assurance e-residency identity scheme that is based on international standards and designed for business and government use, to be conformant with eIDAS. This situation creates a good opportunity for PTER to meet the needs of industry across the EU and beyond, and, if it can offer eIDAS Qualified Trust Services and Qualified Signatures, also support eIDAS requirements.

Linking the EU-Indian Leader's Meeting and PTER to the future of eIDAS would be welcome news to several European interests.

14.3 BREXIT

Brexit is a strong opportunity for PTER. Estonia saw an increase in e-Residency applications after Brexit, but **we expect the real opportunity to be during 2021, after the UK's transition deal ends, and British business owners feel the real effects of Brexit.** The scope for PTER outlined in this document will leave PTER as a logical choice for startups and freelancers in the UK, but also for developed businesses that want to continue to trade in Europe. Marketing for PTER can specifically target the UK, and explain how Portugal can offer a solution to British businesses wanting to continue to have a base in the EU.

The UK is pushing ahead with several digital identity-related initiatives. One of these is a pilot led by the Cabinet Office, to validate passport data in real-time against the UK Passport Office database. Our intention is to include UK passport data validation as part of enrolling UK citizens for PTER as soon as possible.

15. ROADMAP FOR THE LAUNCH AND GROWTH OF PTER

A roadmap leads from the early work being carried out now, through to a fully developed international program.

Phase 0 – Preparation. Now to 1 Nov. Demo users only.

- **Outcomes:**
  - To demonstrate regulatory-compliant leading technologies to register a person and their mobile at High Assurance, and to run an AML/KYC check on a foreign company seeking to create a company in Portugal. Also, confirmation of initial requirements with AMA.
  - To demonstrate PTER enrolment of a UK citizen and validate their claimed passport data against the UK Passport Office passport database in real time.
  - To provide a first draft Business Case and Business Model for PTER, jointly developed by AMA and Start Up Portugal. This will incorporate a gap analysis and interoperability specification with:
    - the national eID card (Cartão de Cidadão - CC),
    - the mobile eID solution (Chave Móvel Digital - CMD) and
    - the Professional Attributes Certification System (Sistema de Certificação de Atributos Profissionais - SCAP).

Phase 1 – Initial operational capability. 1 Nov to 1 Feb 2021. To test and prototype operational users from 50 registered micro and small companies.

- **Outcomes:**
  - Ability to enrol at High Assurance and have a PTER account, then create a company in Portugal, and open a bank account with a Portuguese bank.
  - To develop plans for PTER in Indian, UK, and NL supply chains, including Rotterdam port and two airports.
  - To develop plans for PTER to support KYC/AML checks for account opening and EU regulatory monitoring of payments.
  - To begin discussion with major retail companies for PTER to support safer online purchasing of goods and services.
  - To finalise the PTER Business Case and Business Model, with other supporting documents including a 2-Year Roadmap, GANTT Programme Plan and a strong Communication Plan.
  - To develop a funding plan that would result in PTER becoming self-funding.

Phase 2 – Scale up. 1 Feb – 1 May 2021. Operational users plus 500 registered companies

- **Outcomes:**
  - To launch PTER at the same time as the EU-India Leader's Meeting in Porto.
  - To offer 5-10 new value-add services based on PTER, some government and some industry.
  - To start enrolling individuals onto PTER, and see companies and bank accounts established at scale.
  - To have a significant number of users for each value-added service, and to form a User Group to boost user numbers and value.
  - To enrol PTER's first NL and UK citizens seeking to have a company based in Portugal, particularly for companies affected by BREXIT
  - To establish a customer support service
  - To establish a marketing campaign and outreach capability based on a strong Communication Plan
  - To engage with the EU Council and European Commission

Phase 3 – Full operations. 1 May – 31 Dec 2021. 5,000 companies

- **Outcomes:**
  - To offer 25-50 new value-add services based on PTER, some government and some industry, including examples in section 0 above. Additional examples include: gambling KYC/AML, Covid passport, individual Covid risk management, enhanced notaries' e-Apostille;
  - To enrol PTER's first Indian citizens seeking to have a company based in Portugal.
  - To plan for citizens of other nations, including US, Canada and Brazil, and EU member states.
  - To engage with major international organisations, including UN, WEF[5] and FATF[6].

Phase 4 – Future enhancements. 2022+. 50,000 companies

- **Outcomes:**
  - To offer access to new value-added services in other EU countries, and possibly for EU citizens who are PTER users seeking electronic services in USA. Examples include: validation of person and company qualifications and certifications, share trading, fractionalised property ownership, cross-border tax management, cross-border tariff management, food safety and allergy management, border controls, visitor management systems, building access management, disaster management.

[5] World Economic Forum
[6] Financial Action Task Force

- To support digital transformation in the economy and society, and create greater digital inclusion.

Notes:

- Each phase contains the planning and enablers for the next phase
- Phase 1 could potentially be completed earlier.
- Depending on resource and expertise availability and the approach taken, these timelines could be shortened significantly.
- However, these timelines could be delayed if key government organisations or experts are not available to participate.

15.1 Initial Value Proposition

The initial value proposition in Phase 1 is focused on users establishing a company in Portugal to do business in Portugal. This involves:

- Creating and registering a company
- Opening an online bank account
- Creating an office in Portugal

15.2 Scale-up Value Proposition

The scale-up value proposition in Phase 2 goes further, with increased capabilities in Portugal:

- Registering for company and personal taxes
- Registering with regulators
- Recruiting and employing staff in Portugal and remote PTER holders
- Buying, selling, or renting an office location in Portugal
- Contracting for office and IT services
- Contracting for business and travel services particularly secure invoicing, privacy preserving secure cross-border payments, booking a flight, booking a hotel, car hire booking (and counter-fraud), ordering controlled goods online, allergy management buying food;
- Supporting EU-Indian specific objectives.

15.3 Full Operations Proposition

Full operations in Phase 3 seeks to add significantly more value-added services and, as a result of these new services, grow the user population and registered companies exponentially.

15.4 Future Enhancements Proposition

Phase 4 seeks to turn around PTER so that it supports EU persons and businesses seeking to do business outside Europe. This would increase the PTER population several times.

DIGITAL CITIZEN PERKS

PTER

DOWNLOAD
PORTUGAL

EXTREMELY CHILLED APPLICATION PROCESS

JOIN PORTUGAL'S E-RESIDENCY PROGRAM

STARTUP PORTUGAL

16. STAKEHOLDER PARTICIPATION

The Portuguese Government has provided a strong foundation for the user-government functionality. A further requirement is to develop the user-business functionality to match this, which will have many overlapping features with government. This will enable significant re-use, which will reduce costs and risks, and increase shared benefits.

The following draft table is reasonably correct for Phase 0 to begin now and it can be developed quickly for the later phases.

Phase	Government	Relying Parties	Authoritative Sources	Trust Framework Providers & Identity Providers	Others
0	AMA, Foreign Business, SEF, IRN, INPI, AT, Segurança Social, Banco de Portugal, police, cyber	Two banks	UK	To be confirmed	Regulatory experts KYC AML PSD2 MIFID2, GDPR, eIDAS etc Payments experts Assurance experts
1	Same	+ online retail, insurance, contract services,	NL, India		
2	+ Health, Transport, Buildings + Indian organisations	+ recruiting & staff, transport	Several EU nations		
3	+ other organisations		US, CA, BR		
4	+ other organisations				

We believe this program will rely heavily on a number of agencies and individuals in Portugal. In particular we think it will be necessary to engage closely with the following:

- **stakeholders to help with regulatory space, including data protection authority, the surveillance regulator, the financial regulator, the central bank regulator, the tax authority, the company register authority;**
- **stakeholders from two major banks and the Bank of Portugal;**

17. GOVERNANCE, RISK, AND COMPLIANCE

17.1 Governance

Companies will want to ensure that PTER meets government, regulatory, and international requirements for Governance, Risk and Compliance (GRC). The purpose of governance is to manage risk of all kinds within and across all the major stakeholders, and to ensure compliance with organisational policies. Many of these policies, particularly involving data and information, will be implemented in systemised processes and procedures. So, the governance model will need to consider policies, procedures, and mechanisms, and the people that operate them.

The governance for PTER will need to satisfy industry, commercial, and governmental requirements, so **it needs to operate as a neutral body such as non-profit company, a foundation or a 4th sector organisation.**

This is an explanation from the Fourth Sector Group[7]:

> *The economies in most countries comprise three sectors: the public sector (a.k.a. government), the private sector (a.k.a. business), and the non-profit sector (a.k.a. civil society). But now a nascent fourth sector of the economy is emerging, one that combines market-based approaches of the private sector with the social and environmental aims of the public and non-profit sectors to address pressing problems. Endeavours in this sector, also known as for-benefit enterprises, come in a wide variety of models, from mission-driven businesses, social enterprises, and sustainable businesses, to cooperatives, benefit corporations, and faith-based enterprises, among many others.*

These organisations are characterised as being enablers for common good. **We believe that PETR should probably be a collaborative 4th sector organisation where industry and government can work together for the benefit of Portugal's digital economy and society, and also for its international allies and industry partners.** The Advisory Team can suggest collaborative governance models that work well.

17.2 Risk Mitigation Strategy

The risk mitigation strategy is fundamental to the successful operation of PTER and the delivery of its benefits to organisations, companies and people. Successful organisations depend on high quality decision making, which depends critically on the availability of high-quality data. Data quality metrics will be key to ensuring PTER's success.

Major risks include:

- Compliance risks, particularly due to legislation and regulations;
- Cybersecurity risks, particularly arising from the threats and vulnerabilities to devices and systems, as well as insider threats and collusion;

[7] https://www.fourthsector.org/what-is-the-fourth-sector

- Fraud risks, particularly identity theft, identity fraud, impersonation and counterfeit documents;
- Information risks, particularly the theft, copying or modification of data for criminal gain, and also the failure to ensure high data quality;
- Financial risks, particularly with regard to payments and audit;
- Reputational risks, particularly those that damage the branding and trustworthiness of an organisation, which usually result in significant additional costs and risks to the organisation.
- Opportunity risks, particularly where the organisation misses opportunities to compete effectively or be more effective in the delivery of government services.

As part of the EU Network Information Security Platform (NISP), five standards for digital risk mitigation were identified – ISO 27000 Series for Information Security Management Systems, DE BSI 100 series, EE ISKE, ES MAGERIT and US SP800-53. Typically, they involve five major steps:

1. **Identify** (the risks). Also assess the risks and decide whether to transfer, mitigate or accept them.
2. **Protect.** Put in place protection mechanisms to prevent a successful attack and, very importantly, to provide time for Detection and Response. This is Time-Based Security (TBS).
3. **Detect.** Monitor to detect known and unknown threats and events.
4. **Respond.** Respond to the detected threats or incidents (incident management)
    - To contain the incident or threat and defeat it;
    - To ensure business continuity;
5. **Recover.** Recover to normality.

The e-residency Advisory Team has considerable international experience in information risk management and can help to develop the risk mitigation strategy.

17.3 Compliance

PTER will need to satisfy compliance requirements for many regulators and also to cope with multi-jurisdictionality. The positive news is that, by anchoring to passports, there is already a common baseline on which to build. It may be necessary to have additional checks for some jurisdictions, but this is normal in KYC and AML checks, where organisations and people are checked for 'suitability' in addition to 'identity'. These additional checks also look for Indicators of Compromise (IoCs), which are usually binary Pass/Fail results that supersede any risk score.

17.4 Liability models

As an identify provider (IDP), if your user uses the identity for something they shouldn't have done (outside the policy or terms of reference), the IDP can still be liable to the counter party.

Governments and UNCITRAL have been discussing ways to address this. Meantime, **this is an international issue, for which the current solution is to invoke the Commonwealth Law of Virginia to limit the liability to its proper use.** So, a user will sign to use PTER for these things and these things only.

PTER should state publicly what this identity means - it's LoA 3[8] and been through a LOIP[9] 3 Identity Proofing under international standards with a strong risk mitigation strategy should be acceptable for a list of use cases. (Health, payments, controlled goods, borders (maybe including Schengen eventually), government, corporate, consumer).

17.5 Anti-Collusion and eIDAS

As part of a strategic digital risk mitigation strategy for the EU, DG HOME adopted the Belgian ASINP[10] project as an anti-collusion methodology. ASINP was used to assess the degree of collusion within a government organisation where, for example, an inside employee gives an identity to someone who shouldn't have it – and to prevent it. **PTER and the Portuguese authorities will want evidence from other governments that they have appropriate anti-collusion measures in place and their risk mitigation strategies support LoA 3 and LOIP 3, or higher.**

Additionally, if PTER is eIDAS "notified", then that liability model would be included, however **eIDAS is for public use, not commercial, so the liability won't cover commercial operations.**

[8] Level of Assurance – defined in ISO 29115: Entity Authentication Assurance Framework
[9] Level of Identity Proofing – defined in ISO 29003: Identity Proofing.
[10] Strengthening Architectures for the Security of Identification of Natural Persons in the EU (ASINP)

18. BUSINESS MODEL

Working with AMA and others, the Advisory Team can help to build both the PTER Business Case and PTER Business Model.

As digital transactions increase and individual transaction costs reduce, so **the cost to enrol in PTER and also to use PTER to authenticate must also be low enough to be affordabl**e. If it is done right in a way that is highly reusable across multiple use cases, the costs are low and quickly affordable; **this means leveraging existing high assurance solutions rather than trying to build a completely new PTER infrastructure**, with all the costs, risks and delays that would be involved.

A key change is the commercial move away from "the customer pays" to "the Relying Party pays." It is the Relying Party who provides the services to the customer either because they need to do so e.g. to pay taxes, or because the customer wants a commercial service, such as KYC or AML check with a bank, where the bank pays. The more the customer uses PTER, the lower the per transaction cost becomes.

The Estonian e-Residency charges each user €100 for three years, however the transaction rate is low and most of the Relying Parties are government departments. So, it is understandable that the Estonian government wants to pass most of the costs on to the user. However, for PTER, we envisage government use being relatively small and much less than commercial use. Consequently, PTER will need government funding to get started with government departments and a few banks, but thereafter PTER's focus should be to build up the commercial and cross-border use so that **PTER rapidly becomes a wealth generator. We envisage the cost to the customer being €10 or less per year. PTER should be the best value for money e-Residency available anywhere.**

The Advisory Team can help with different funding and payment models. Two methods of raising funding and managing payments are often used:

Pre-payments. Known as "Pre Pay" in the USA, pre-payments involve a small group of major Relying Parties paying several years' subscriptions in advance in return for a discount. A theoretical example would be a bank paying €400k up front for 5 years' subscription of €100k/year, for a notional 25k/year PTER KYC authentications. This is a cost saving of 20% for the bank, but it gives the PTER organisation €400k starting capital. (For such a bank, PTER would also improve the detection of bad transactions and reduce manual operating costs, saving €10-100M+/year). Having ten such pre-payment customers would give €4M startup funding, which would go a long way to meeting the startup and scale up costs for a year or two. This reduces costs to the government.

- **Credits.** Users and Relying Parties pay in advance for credits to use PTER, so PTER doesn't have to bill or chase any customer, and it avoids any legal or financial disputes. PTER operates a credit-based account, not a debt-based account. Users and Relying Parties "top up" their credits.

19. CONCLUSIONS

1. The Portuguese government and AMA have established a strong, coordinated approach across the Portuguese government for PTER, which will make it much easier to collaborate with other governments, industry and the EU.

2. There is a unique opportunity for Portugal to launch a form of e-residency that goes far beyond what other countries have developed and are considering.

3. PTER's success will depend on creating a marketplace that can create, use and re-use PTER in a safe, secure and affordable manner. To be resilient and cope with change, this will require a federation models where CC, CMD, SCAP and other high assurance capabilities each have a role to play to support identification, authentication, digital signatures, encryption and non-repudiation, which are the primary uses of digital identity.

4. Startup Portugal provides an initial industry focus for PTER, from which a team will need to be formed with the experience, capabilities and capacity to plan, operate and grow PTER for use across a wide range of use cases.

5. PTER's success will depend on meeting industry requirements at scale and being responsive to new requirements and change. This particularly includes meeting regulatory requirements for High Assurance (LoA3) identification, authentication, and trust services.

6. PTER should be based on regularly validating passport data, as passports are the de-facto global identity document, augmented by other credentials where appropriate, notably citizen e-IDs and eIDAS.

7. PTER must comply with increasingly demanding regulations for privacy, KYC, AML and cybersecurity, which will require Privacy Enhancing Technologies and the use of alerts, such as push notifications.

8. PTER will be a high assurance digital identity that complies with international treaties and standards, it could be developed into a revenue-generating service used by global businesses for a wide range of activities:
    - PTER could be used by foreign businesses to establish a legal base in Europe to manage trade in and out of the EU
    - PTER could be used by international banks to support KYC and AML during account opening, account monitoring and for approving cross-border payments
    - PTER could become a digital trust service people use in many places, for example, to open a bank account in the UK, establish a business in Delaware, or monitor the flow of controlled goods through Rotterdam

9. AMA can re-use PTER to enable non-Portuguese citizens to access government services to register a company and pay taxes, and potentially use digital services for Portuguese citizens.

10. Most of the technologies and best practices needed to implement PTER already exist and can co-exist in the PTER marketplace. PTER will need a collaborative governance model for this.

20. RECOMMENDATIONS

1. AMA and Startup Portugal should engage in informal, expert discussions to outline a suggested scope for PTER based primarily on customer requirements.

2. AMA and Startup Portugal should initiate the steps in Phase 0, to help inform all parties on best practices relevant to PTER and using PTER.

3. AMA and Startup Portugal should begin to develop key documents – a PTER strategy, business case, business model, outline design, Privacy Impact Assessment, risk assessment, resource plan, and roadmap that together reflect both government and industry requirements and inputs. This should re-use CC, CMD and SCAP where appropriate.

4. AMA and Startup Portugal should develop a stakeholder map across government, regulators, industry sectors (national and international). PTER should engage with stakeholders to document government and major industry requirements for PTER, and compile these into a Catalogue of Collaborative Requirements for High Assurance. This should include benefits to Portuguese companies that re-use PTER services.

5. AMA and Startup Portugal should identify and prioritise national passport offices, citizen e-identity and eIDAS notified identity schemes as potential authoritative data sources for real-time identity data validation.

6. The Advisory Team, with Startup Portugal, should use existing industry relationships with the State of Delaware to explore interest in using PTER to support business from Delaware-registered companies to Portugal and Europe, and vice versa.

7. The Advisory Team, with Startup Portugal, should use existing industry relationships with Dutch authorities and industry to explore interest in using PTER to support trade through Rotterdam.

8. AMA and Startup Portugal should use existing relationships with the European Commission DG CNECT to identify synergies with eIDAS, EBSI and ESSIF.

9. AMA and Startup Portugal should begin developing a marketing campaign and marketing capability to reach out and encourage Relying Parties to provide services that need PTER, end user organisations that use PTER, passport offices to provide authoritative data validation for PTER and foreign governments to participate in PTER.

10. AMA and Startup Portugal should develop a draft collaborative governance structure that covers all necessary areas of governance to meet regulatory and business requirements.

NO PHYSICAL ATTENDANCE NEEDED

DIGITAL CITIZEN PERKS

DOWNLOAD
PORTUGAL

PTER

JOIN PORTUGAL'S E-RESIDENCY PROGRAM

STARTUP PORTUGAL

APPENDIX 1 - GAP ANALYSIS RELATING TO AMA PROPOSAL

A simple, initial gap analysis with the Initial AMA documents has been developed; it does not reflect new work by AMA and partner organisations. The AMA has a good and aggressive roadmap that will help drive the development of the PTER to meet Government requirements, enabling user to government interactions such as establishing a company or paying taxes. The Advisory Team can develop a roadmap to meet the industry, national, and international customer requirements. This includes leveraging new technology best practices and meeting EU regulatory requirements that affect all online businesses. These regulations will significantly strengthen the business case and the customer demand for PTER.

The gap analysis informs the necessary future work, including immediate foundational steps, a pilot to test business benefit, the PTER trust framework based on international standards, the business case based on international user requirements, and a high-level implementation and communications plan. This will include integration and interoperability tables so AMA's development to meet government requirements efficiently will match and fit with the requirements of the other key stakeholders. Key requirements and key risks will be analysed with options to address them.

Slide	Key points	Requirements
3	Digital by default. Greater access to public services	PTER supports and extends digital by default We do not believe it is necessary to meet consular or other people to enrol the identity and conduct high assurance identity proofing Opening a bank account is a private sector action and requires the financial regulator to allow banks to open accounts remotely for people using the PTER. This will require the financial regulator to work with AMA and with the banks. We need to examine which of the public sector activities listed currently require notarisation. It should be possible to do all of these things without a notary, particularly as many countries no longer use notaries for identification purposes.
3	Measure description	PTER will leverage EU certified high assurance remote enrolment, not face-to-face, which is weaker
5	Three main sections	Identification/identity proofing and authentication are foundational. For risk mitigation and regulatory compliance, business requires authorisations based on Suitability checks (also known as vetting), digital signatures, encryption and binding to organisations for legal persons. For mobile and IoT, this requires device bindings also. From a risk, security and legal perspective, highly re-usable best practice capabilities already exist, which autenticação.gov will need to include, if PTER is to be widely adopted. We suggest that the identification and authentication processes area designed in a way that the processes and infrastructure can be shown to other parties when necessary. Transparency of the process will allow other countries and entities to evaluate how reliable and trusted the identity and the trust processes are. This will be essential to work with, for example, the American government, and other global Relying Parties.

6	Government areas in iSimplex 2019	This is an excellent level of engagement and provides a very strong foundation. Centralising on CMD runs counter to a federation and data validation models. It is likely that some authoritative sources and other governments will be unwilling to allow copying of personal data under GDPR and international law. This area needs further discussion to agree a modified approach that meets policy and stakeholder requirements. eIDAS will be useful to identify some EU citizens, but it is designed for citizen to government identification, not citizen to citizen or business. This impacts the liability models. We anticipated using eIDAS in support of a passport to identify a new EU user. We also expect to develop a list of countries that allows people from 'safe' countries to do more with eIDAS than others. This protects Portugal from identities issued by European countries with higher levels of corruption where someone can obtain a genuine identity token based on a fake or stolen identity.
7	Segmentation	See above about eIDAS. We think it will be essential for individuals to use a passport, potentially combined with other forms of verifiable identity. We recommend that PTER will validate claimed passport data with the issuing country's passport database to ensure it is current at the date of validation, and also how often that database will be referenced in the future so that any identification token created by PTER or the passport authority is valid. This addresses the situation where somebody uses passport to create their PTER, and then their passport is stolen the next day, or someone using a passport that has been stolen but not yet reported. Consider that not all countries have a 'fiscal number.' The information we require from people either has to reflect what each country has, or be universal for all countries. This may need some data attribute mapping between nations. For non-EU, the same issues apply: will you check the issuing country's passport database, and how will the authority keep the token updated? This can be done today.
8	Why Portugal	These are all good offers, but they are what Estonia has, and will be what other countries will have soon. We need to plan ahead for some bigger advantages for PTER Portugal. The opportunity over other countries will focus on the assurance level of the identity, and the ability of Relying Parties to verify how secure the identity is in real time. With a high assurance level identity that foreign regulators can verify, the Portuguese e-resident and their company will be able to do more, and on a bigger scale. not just freelancers but larger corporates. Example: if Portuguese e-Residency could be used as a form of identity at Rotterdam port to manage freight, non-EU companies could use Portuguese companies to import to Europe. This would require the underlying ID, and the company, to pass international regulatory standards.
9	Channel, identification, attributes	As outlined above, enrolment/identification should all be done online, without needing the passport channel as described. eIDAS alone doesn't work for several reasons. The focus should be on passport + other factors or evidence The data attribute list needs to correspond with whatever the applicant has from their country. The list may need to be different for each country.

10	CMD eIDAS	With CMD you will also need to ensure it works with mobile operators in other countries, otherwise e-residents will have to get a Portuguese SIM card. We believe eIDAS will be difficult for foreign nationals because it is not intended for commercial use, only citizen-government. eIDAS is not accepted commercially in most of Europe and is not sufficient for a KYC or AML check. The eIDAS credential is only as secure as the document it is based on, which is not secure if the issuing country has high levels of corruption. To protect Portugal from organised crime, etc, we propose not allowing all eIDAS automatically to create a Portuguese e-resident identity. The problem here is if criminals from corrupt EU countries use fake IDs to create a Portuguese ID, then Portuguese e-residency will lose trust from Relying Parties and users. However, we do recommend notifying PTER under eIDAS so that the Portuguese e-residency becomes a pan-European ID for public purposes. This will give it a significant advantage over other e-residency offers. NOTES: We note that Digital Mobile Key (CMD) is a means of authentication and digital signature is certified by the Portuguese State. It allows the user to access several public or private portals, and to sign digital documents, with a single login. Therefore PTER will need to be CMD compliant for users to access Portuguese government services. However, PTER will need to have other credentials to be able to operate internationally and commercially. The Digital Mobile Key associates a mobile phone number with the civil identification number for a Portuguese citizen, and the passport or title / residence card number for a foreign citizen. This means that the passport information for all PTER customers will be held in the DMK, which is likely to create legal, liability and technical issues, as the same bindings will have to be made in commercial identity systems supporting PTER. A federation model may get over this problem.
11	For business section is required to define how to enhance "doing business" and business attractiveness.	Most of these requirements are just for interactions with the Portuguese government. Doing business requires a much greater list of commercial requirements that result in daily use, which makes PTER more attractive and beneficial.
12	Light and Premium access	There is no commercial regulatory use for Light Access. The business security target is Level of Assurance 3, which should underpin Premium Access.
13	Cluster diagram	We are unable to relate this to existing major industry requirements.

14	Different levels of maturity	Most of these are consumer or business to government services. For the e-residency to be useful in business, we also need a similar map of actions companies need to be able to do locally, in Europe, and internationally. The business case for e-residency is not that people can do business with the Portuguese government, but that they can use that company to do business with other individuals and companies, in Portugal, the EU, and internationally. The Relying Parties in the first case are all Portuguese government agencies, or in Portugal, so they will have a high level of trust for the system. The real value will be if Relying Parties outside Portugal, both government and commercial, believe that the Portuguese e-residency has a strong enough trust and liability model that they can make contracts, complete KYC, and base transactions on the ID. For that, the ID has to be both very safe, constantly checked against multiple Issuing Authorities, and transparent so people can check why it is safe. For example, if a British person creates an e-residency with a passport, the system would cross reference with the UK passport agency when the identity is created, and would either check the passport database regularly, and / or check it live each time certain significant transactions are made using that ID. This would protect against loss, theft, or fraudulent use of the passport. This would need to be replicated with multiple countries, and multiple Issuing Authorities. It is likely that the core Portuguese ID system would have an open API that multiple private sector identity companies can use to check credentials in both directions for Relying Parties. This would create an ecosystem of identification around Portuguese digital identity that would be of great value to all the parties involved.
15	Government support for digital services	We do not fully understand this chart. We welcome the opportunity to discuss it, particularly in relation to e-Codex for lawyer signatures.
16	Roadmap	This describes the technical work in Portugal, but does not describe the business case. Just because it is launched, does not mean people will use it. The problem with Estonia was that a lot of people registered for an ID when it was launched just to see what it was, but then never used it. We propose working in parallel on the business cases, and marketing strategy, so that people start to use it to establish companies and do business. See previous notes about the difference between government and business use cases. From this we can quickly create a roadmap. A suggested Phase roadmap is in the document – we would like to discuss this with AMA. We look forward to discussing this slide and understanding the latest situation.
17	Stage 1 Cluster A	This slide requires further discussion to understand the latest situation.
18	Stage 2	This slide requires further discussion to understand the latest situation.
19	Ministry interactions	This slide requires further discussion to understand the latest situation.
21	AT	This slide requires further discussion to understand the latest situation.
22	IRN, IGFEJ	This slide requires further discussion to understand the latest situation. IRN is particularly important for business.
23	Segurança Social, Instituto de Informática	This slide requires further discussion to understand the latest situation.
24	Banco de Portugal	We recognise the great importance of the Bank of Portugal to business and to PTER. We look forward to discussing this slide and understanding the latest situation.

APPENDIX 2 - DETERMINING LEVELS OF ASSURANCE AND LEVELS OF IDENTITY PROOFING

International standards and best practices continue to evolve in response to the changing strategic situation and regulatory imperatives. ISO 29115 Entity Authentication Assurance Framework (EAAF), ITU-T X.1254 and US SP800-63 are all similar in their approach and structure, based on four graduated Levels of Assurance that should match to the Relying Party risk appetite and strategy, which are the outcome of the EAAF and similar. Several governments base their policies on these standards, for example, the UK government's Good Practice Guide 45[11].

The EU's eIDAS Regulation is similarly based, however it does not adequately support the highest international Levels of Assurance. If PTER were compliant with these international standards then it is possible that PTER could be "notified" under eIDAS, which would result in an PTER credential being accepted by every other EU nation for public digital identification purposes, by EU law.

			Management Organizational
Enrolment phase	• Application and initiation • Information verification	• Record/keeping/ recording • Registration	• Service establishment • Compliance
Management phase	• Credential creation	• Credential suspension, revocation, and/or destruction • and/or replacement	• Management and audit • Components • Infrastructure • Capabilities
Authentication phase	• Authentication • Record-keeping		

Figure 1 - Overview of the Entity Authentication Assurance Framework

An overview of the EAAF is shown in Figure 1, which is from ISO 29115. Not all elements are required in all situations, however it is important to distinguish between:

- The Enrolment Phase, which includes identity proofing. Identity proofing is not a one-off initial activity, but a **continuous activity, driven by the risk mitigation strategy and the Common Policy.** It contains the identity management lifecycle, including revocation i.e. death.

[11] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

- The Credential Management Phase, where its lifecycle is managed. This includes all functions and credential types e.g. for authentication, digital signatures, secure email, encryption, whether in software or hardware.

- The Authentication Phase. This involves the use of the credential to authenticate to prove that the entity or person is who they claim to be. Monitoring the use of authentication is another **continuous activity, driven by the risk mitigation strategy and the Common Policy, which reflect Relying Party risk.**

The risk model in the trust framework for any identity system depends on the business use cases and the Relying Party risk appetite. ISO 29115 describes the use of identity credentials for authentication, based on four Levels of Assurance (LoA), which reflect the risks to the Relying Party.

- **LoA 1 (Low Assurance)** assumes little or no confidence in an identity or credential and contains no meaningful identity information e.g. an email address. The main use of LoA 1 is for social media, where users may have many accounts and identities.

- **LoA 2 (Medium Assurance)** assumes some confidence in the identity or credential based on a government issued identity document. The main use of LoA 2 is for consumer activities, where banks and businesses have requirements to satisfy increasingly demanding Know Your Customer (KYC) and Anti-Money-Laundering (AML) legislation. The risk model assumes that all risk is financial and, in the event of failure, compensation and insurance are sufficient. Unfortunately, this opens up opportunities for fraudulent claims. **Hence the EU Payment Service Directive 2, which requires Strong Customer Authentication (SCA) that approximates to LoA 3.**

- **LoA 3 (High Assurance)** assumes high confidence in the identity or credential, based on government issued identity documents and other information and checks. The main use of LoA 3 is for organisational employees in industry and government, but financial regulations affecting individuals are increasingly moving to LoA 3. The risk model is more complicated, particularly regarding the protection of intellectual property and privacy data, and is focused on preventing an identity management failure.

- **LoA 4 (Very High Assurance)** assumes very high confidence in the identity or credential, based on government issued identity documents and other information and checks. The use of a hardware token and PKI cryptography are mandatory. The main use for LoA 4 is the situations of high economic risk, danger to life and national security.

LoA reflects the outcome-based perspective. The input-based perspective is reflected in the Level of Identity Proofing (LoIP) defined in ISO Technical Specification 29003 – Identity Proofing. This states:

> *The proofing party shall perform identity proofing in accordance with a documented identity proofing policy. The identity proofing policy shall state, as a minimum:*
>
> - *the LoIP(s) at which the identity proofing service is offered;*
> - *the jurisdiction in which the identity proofing service operates and in which it is offered, and the applicable legislation;*
> - *the intended context for which identity proofing is being undertaken;*
> - *whether identity proofing is in-person or remote;*

- *what identifying attributes applicants are required to provide;*
- *which evidence of identity for the identifying attributes shall be used as authoritative evidence and which as corroborative evidence, when verifying proofing information;*
- *what are the possible outcomes of the proofing operations;*
- *how the results of the proofing process will be communicated to the applicant or appropriate parties;*
- *what records of the proofing processes will be retained, by whom and for how long.*

In any identity proofing process, the user presents Evidence of Identity (EoI) with the application, and the authority normally checks additional Authoritative and Corroborative Sources without involving the user, in order to reach a registration decision.

Based on the EoI, ISO 29003 contains three LoIPs:

LoIP	*Description*	*Objective*
LoIP 1	*Low confidence in the claimed or asserted identity*	*Identity is unique within the context*
LoIP 2	*Moderate confidence in the claimed or asserted identity*	*Identity is unique within the context* *and* *some processes are undertaken to establish the identity exists** *and* *the subject has some binding to the identity.*
LoIP 3	*High confidence in the claimed or asserted identity*	*Identity is unique within the context* *and* *strong processes are undertaken to establish the identity exists** *and* *the subject has a strong binding to the identity.*

** The concept requires the values of the identifying attribute to match that of a record in the evidence.*

In all cases, the identity has to be unique within the context of the system(s). This raises challenges in special situations where a person requires two identities for legal or security reasons. The Advisory Team can discuss this further.

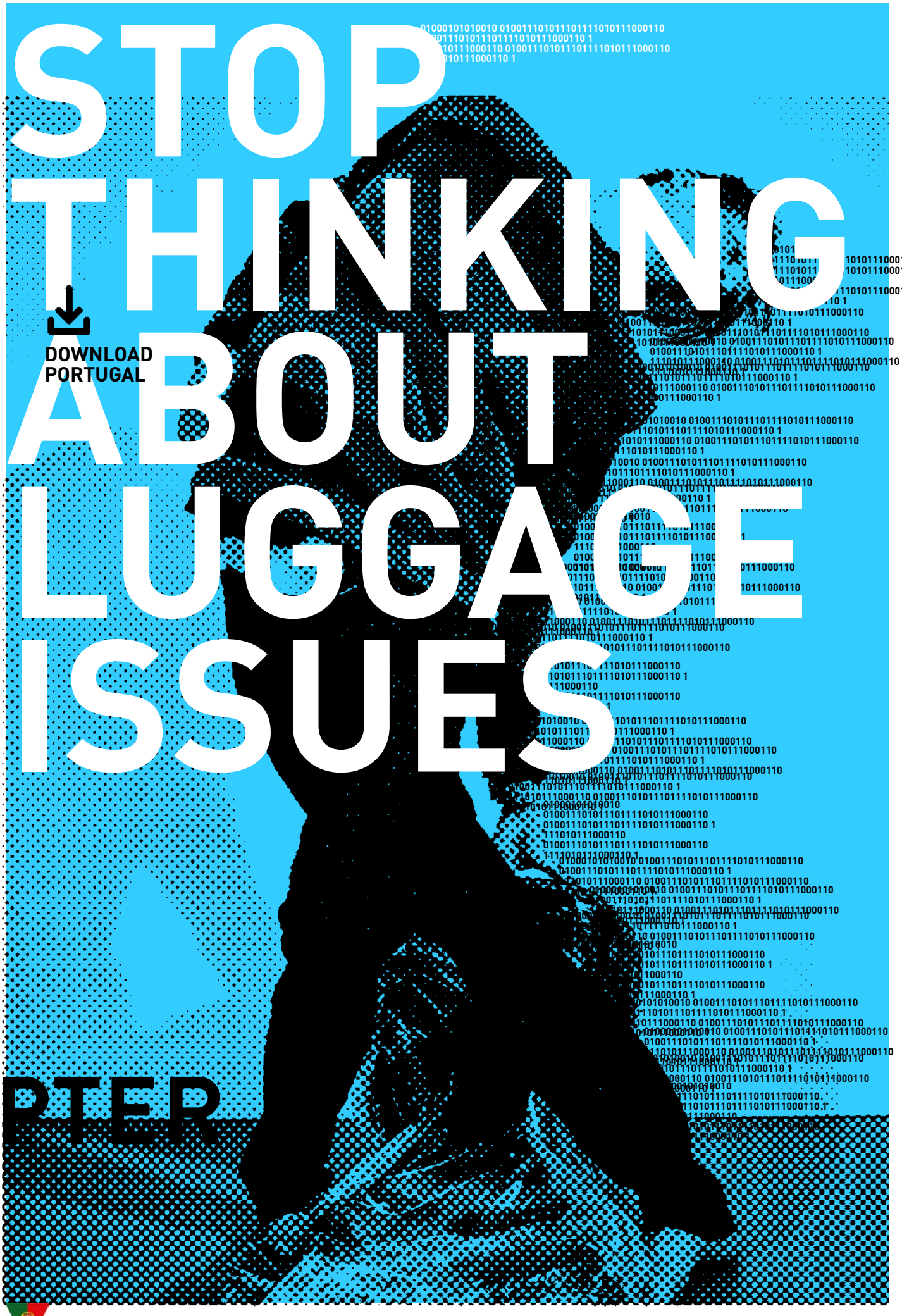
The LoIP is a combination of the existence of the identity and the binding of the identity to the person. The differences between LoIP 2 and 3 are that:

- LoIP 2 shall verify that the identifying attributes exist in corroborative evidence but that LoIP 3 shall verify that the identifying attributes exist in authoritative evidence.
- LoIP 2 shall check the binding to the identity using one factor. LoIP 3 shall check binding to the identity using two or more factors.

Both of these are continuous activities, driven by the risk mitigation strategy and the Common Policy, which reflect Asserting Party (the attribute authority) and Relying Party risks.

One of the Advisory Team is the ISO co-editor of 29003 and also the UK national expert for 29115, so the Team has significant knowledge and experience in the use of these standards in government and commercial implementations.

In conclusion, to meet industry business and regulatory risks, PTER must support LoIP 3 for identity proofing and LoA 3 for authentication.


STOP
THINKING
ABOUT
LUGGAGE
ISSUES
DOWNLOAD
PORTUGAL
PTER
JOIN PORTUGAL'S E-RESIDENCY PROGRAM
STARTUP PORTUGAL