Emerald TrustXchange

Enabling Trust in everyday interactions on the island of Ireland

Vision Whitepaper

Version 1.3

May 2020

Disclaimer: this paper reflects the vision for the Emerald TrustXchange. Not all capabilities are confirmed, nor or all scenarios or participants. This reflects a future state desire and the focus is to work together collaboratively to make this vision a reality. References to businesses and Government are purely for illustrative purposes

Contents

Introduction

Here in Ireland, as in the rest of the world we are increasingly living our lives digitally. When we conduct business online we can do everything from weekly shopping, booking airline tickets, taxing our cars, applying for a mortgage or simply signing up for gym classes.

The online activities with the highest value are often those where we need to supply verifiable personal information. Because the gathering of this data is cumbersome due to a lack of single sources and common standard, these higher value transactions are also those with the poorest customer experience, cost business more to administer and often exclude or deter many from enjoying the benefits of the online market as they can't satisfy the requirements.

Providing verifiable information is essentially proof that we are who we say we are: proof of identify, proof of address, proof of qualifications and so on. Typically, this is achieved through physical documentation that then needs to be seen, examined and even felt to confirm their bona fides: that they are indeed the genuine article.

In years gone by, the difficulty of easily producing a high-quality counterfeit copy of a utility bill was enough to convince us that any bill presented was more likely than not genuine. Nowadays the bill is issued electronically and printed at home if required as evidence. Unfortunately, it has become easier to alter or create a fake bill so this home-printed copy is rarely, as the cliché goes, worth the paper it's printed on.

It is the **trust** we place in the utility bill, a passport or an employer vouching for us that allows us to complete financial and other transactions with other people and organisations. Without that trust, there is nothing. In the online world it is costly and inconvenient to exchange physical documents and in the physical world it is becoming more difficult to trust documents: how can we be sure they haven't been altered? How can we be sure they belong to the person presenting them, or if they have been revoked since they were issued?

Many of the documents or artefacts we want to exchange are those that identify an entity (e.g. a person or a place or a thing), or some attribute of that entity, and are typically called **credentials**. For now, let's just consider *credential* a fancy name for an important document like a passport, driving licence, utility bill, exam results: you get the idea!

What if, instead of relying on physical copies of credentials we had:

- A digital copy stored in a trusted and secured location;
- Whose sharing and use were at our sole discretion; and
- A verifiable copy of which we could share with a third-party for a particular purpose and that purpose only?

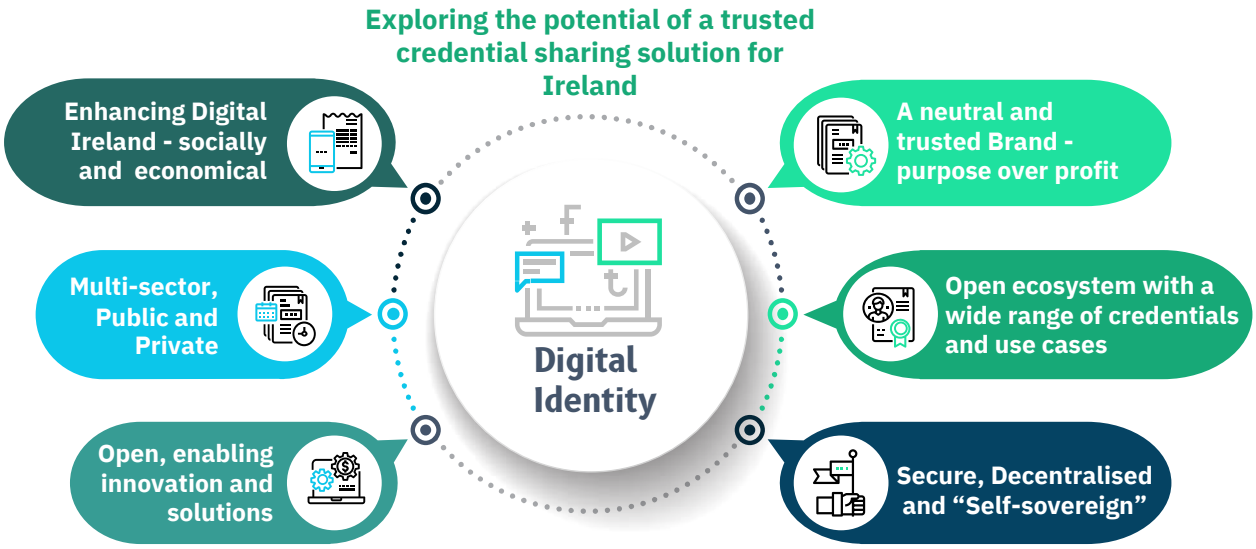
Emerald TrustXChange is a not-for-profit organisation whose mission is to provide a secure, scalable and privacy-respecting way for exchanging digital credentials for the island of Ireland. The motivation for doing this is to make it easier for us as citizens and businesses to do business and conduct daily life both online and in-person, for more of our fellow citizens to enjoy the digital economy and for businesses to benefit reciprocally.

Raising the trust bar in our country would reduce fraud, crime and generally make life better for all of us by widening access, reducing "friction" and improving customer experience and taking unnecessary time, steps and 'waste' out of online journeys. Through the creation of the ecosystem,

standards and mechanisms to securely store and share credentials, **Emerald** is setting out to enable and connect the dispirate credential paradigm that exists today – it is not intended to replace any current or planned identity scheme or initiative, merely to connect them for collective betterment, and create the platform for identity innovation.

The World Economic Forum estimates that solving the identity problem could add 3 – 13% to the GDP of the country - while Ireland is probably at the lower end of this scale given we are a mature, open economy and strong digital adopters, the economic benefits are not to be sniffed at, and staying at the forefront of the digital economy is critical for our continued success.

As illustrated below, to enjoy these benefits, at scale and consistency, Ireland needs a multi-sector and public-private partnership to come together and build the mechanisms, standards and trust framework to remove 'verification' as the pain we all know it to be. This is a grand task, and will take perseverance, imagination and higher purpose willingness. This probably all sounds a bit theoretical? Difficult ? Or even unachievable ? Well before we unravel those questions, let's imagine how it might work in practice.



Trust in Everyday Life

Renting a Home

The **Emerald TrustWallet** is a free app that works on iOS and Android mobile phones. Let's imagine for a minute that it contains a digital copy of Fred's driving licence, some recent bank statements, utility bills, a certificate of employment and a P60. We'll explain later how they got there.

Fred is new to Dublin and is about to rent an apartment from Susan's Rental Company. He's heard about scams where fake landlords steal deposits for properties they don't even own.

Fortunately, both Fred and Susan have **Emerald TrustWallet.** Fred scans a QR code which Susan shares from her Landlord App and sends Susan his confirmed name and address which is verifiable from his bank statement, and his PPS number and employer name which is sourced from the P60. Susan can be confident that the bank statement was actually issued by AIB and the P60 was issued by the Revenue Commissioners and can therefore trust the information being presented.

Underneath the covers the digital credentials are using similar encryption and digital signing technologies to those used in a web browser when we type in credit card details that travel securely over the Internet from our homes to the business we are dealing with.

The details are combined for Fred into a new credential marked with the description "Provided to Landlord for Rental Property", that retains details of where the individual pieces came from, who they came from and are encrypted for Susan's use only.

By return Susan provides Fred with her corresponding details, such as Name and Address and issues a receipt for the deposit he has just paid in the same manner and to the same benefit.

We call this 'digital credentials exchange', and it supports a number of important principles:

- **Self-Sovereign:** One of the key principles of the solution is that the credentials are held by the person to whom they were originally issued to, and it is only with their express permission that they are shared. Typically they are stored securely on a device like the person's smartphone rather than somewhere centrally where they could be stolen or mis-used.
- **Non-repudiation:** basically neither Susan or Fred could later pretend that they didn't provide their credentials to each other. The credentials are *signed* in a manner that shows that they were present, provided the credentials and consented to do so.
- **Confidentiality:** the credentials are encrypted by the receiver and stamped with the purpose and who provided them - this can be traced with certainty, but also restricted for use in any other purpose or onward sharing.
- **Security:** it becomes very hard to intercept or view the data without permission as the data can't be used without an approved app/device and 'keys' issued by the data holder and the data receiver involved in the data transaction (i.e. on its own, stolen data is useless – making it less attractive to hackers).
- **Integrity:** the credentials also contain a *hash* or *digest***,** a clever mathematical summary that can be used to prove that the content has never been altered in transit or since inception.
- **Privacy:** only the provider and the receiver know what has been shared and when, meaning that there's no correlation of the person across contexts (the Revenue Commissioner or the

bank don't know – and can't find out - every time you rent a house or use the credentials they gave you; just like it is today with paper copies)

- **Openness:** there's no single, central authority who can see all the data, or who can turn the system off. It all works because the data is shared peer to peer – just like we share paper today. So there can't be any 'lock in' to one technology, provider, government department or indeed any one organisation. Everyone can choose which technology they want to use, meaning that the ecosystem is open by design. Every bit like the Internet.

So there is a secure chain of trust between the original P60 credential issued by the Revenue Commissioners to Fred, and onward from Fred to Susan. Susan can verify with certainty that the PPS number and employer name came from the P60 issued by the Revenue, even though Fred is the one providing them. As Fred's credential is marked for a particular purpose Susan wouldn't be able to pass it on to a third party pretending that it is actually hers.

So far so good.

Now Susan goes to the Residential Tenancies Board to setup the new Tenancy and she's able to transfer the details directly from her **TrustWallet** into the RTB system and/or ask Fred to do so if they haven't already agreed this in the original transaction. What's more the RTB system can also see the lineage (or source) of the credentials so can have high confidence that a PPS number supplied on a Revenue Commissioners P60 is legitimate and matches the name from the same source.

This simple example:

- Facilitates and enables trust between two complete strangers;
- Demonstrates how individuals can share data in a fast, easy, secure and private way, under their control, anywhere and at any time;
- Makes attempted fraud a high-risk and unlikely endeavour; and
- Provides onward trust and certainty to any downstream agencies who need to rely on the data.

Let's take a look at another example.

New arrivals in Ireland

Alberto Russo, based in Rome, accepts a job offer from Google in Dublin.

Alberto is registered for identity purposes with InfoCert who are a certified eIDAS participant, operating digital identity services across Europe. eIDAS is an EU federated-login standard which provides a high bar for the initial verification of the person when registering with the chosen eIDAS provider, and developed to support a single European Digital Market.

InfoCert and other eIDAS providers agree to issue an **Emerald**-compatible version of Alberto's eIDAS credential, therefore providing a cross-border credential containing name, date of birth, nationality and perhaps national ID number[1]. This is stored in Alberto's **Emerald TrustWallet.**

His new employer, Google, also issue a credential providing proof of Employment and salary level, again stored in Alberto's **Emerald TrustWallet -** these credentials are adequate to support Alberto in opening a Bank Account, renting a new home and connecting utilities for respective business that

[1] The use of the national identity number (e.g. PPSN in Ireland) is restricted to specific purposes in some jurisdictions.

leverage the **Emerald** solution, and benefiting every party in these transactions in what is often a tricky and frustrating process.

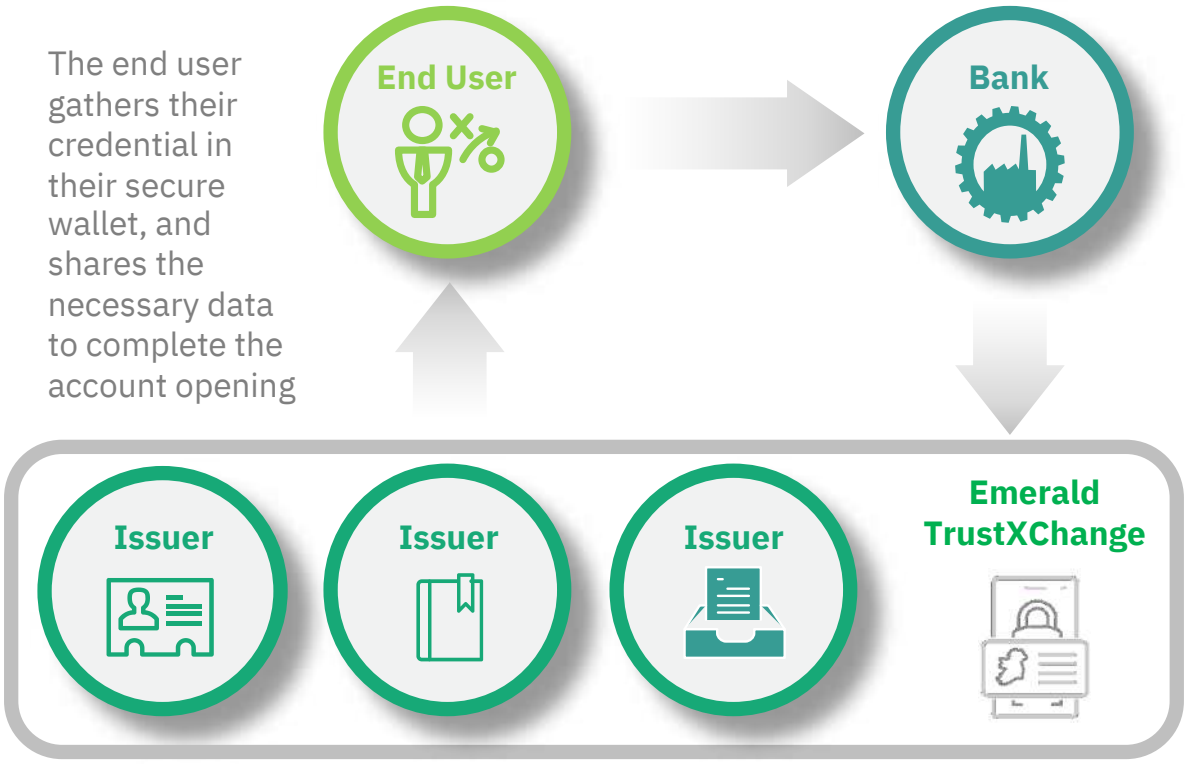
Know Your Customer

To now look at how the **Emerald TrustXChange Network** supports businesses, let's take a look at the obligations on Financial Institutions and the regulation they are bound by to know who you are before they do business with you, called Know Your Customer or KYC.

To open a new account or product, in addition to all the personal information normally required for a new relationship, typically the Bank is mandated to gather, verify and store:

- A Government-issued photo id: typically, a passport, passport card or a driving licence
- Proof-of-address: typically a utility bill or a bank statement, issued within the last 6 months

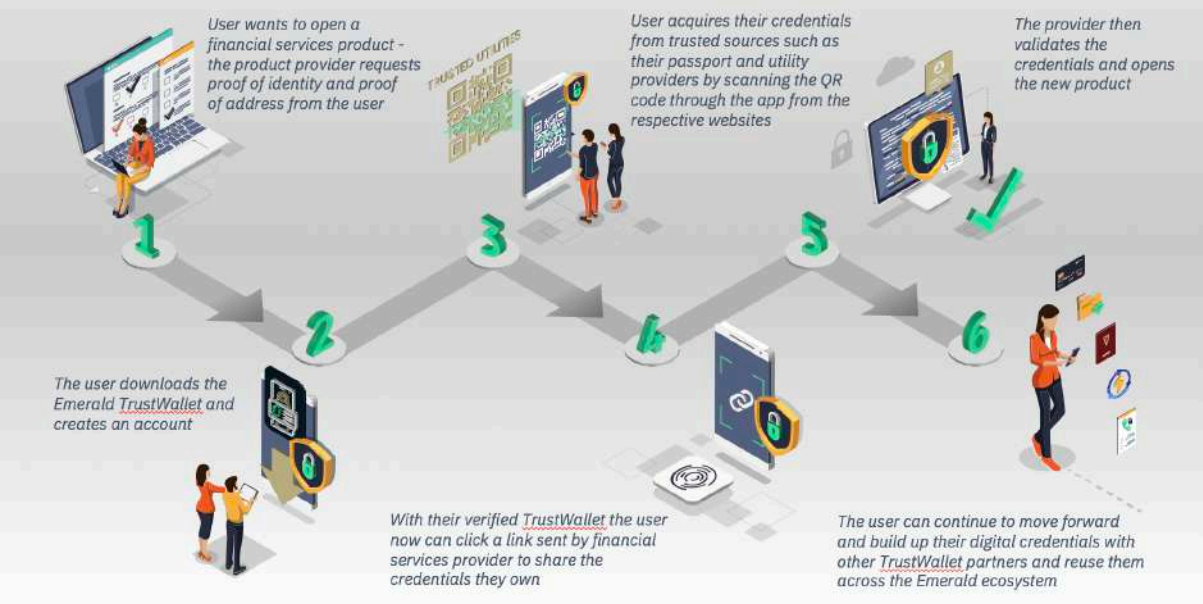
What if Banks and other financial institutions could integrate with the **Emerald TrustXChange Network**, allowing them to exchange credentials directly with individuals and integrate the data from those exchanges into automated business processes. In these exchanges, the Issuer of credentials is the Government or Utility Provider, the Owner is the individual and the Verifier is the Bank (see illustration below).



Source: https://cryptocalibur.com/wp-content/uploads/2018/06/sovrin-ico-600x278.png

Utilising this 'trust triangulation', the end consumer can simply scan a QR code or link on their desktop computer or click on the institutions mobile app when onboarding and exchange the necessary KYC credentials and indeed broader attributes or personal information that the

application requires, all from the **Emerald TrustWallet** and as a result satify the Bank's requirements, and make for a smoother journey for all parties. It's as simple as 1,2,3 … and certainly simpler than it is today in many cases. Have a look at the user story below to help bring that to life.



Logging on to an online account

Research indicated that the average internet user has 92 online accounts, and is likely to have over 200 by 2020 – this sounds very familiar to all of us, as does the accompanying frustration with trying to remember each and every set of login usernames and passwords, not to mention the associated costs and security challenges with resetting gorgotten passwords etc. Simply embedding, a "Login with **Emerald**" button on a website would allow Fred to login, request an appropriate **Emerald** (or indeed eIDAS) credential and allow immediate access to the site and service.

Because **Emerald TrustXChange** isn't an identity system in its own right – instead it's a set of standards and protocols, like HTTP or TCP which can be leveraged universally – this means any entity can issue or check digital credentials, to anyone at any time. These can be high-quality credentials issued by Government (MyGovId), eIDAS, a Bank or Financial Service company.

These same credentials can then be used for *logon* to websites or applications where that application chooses to support it. The experience would be similar to the *Login with Facebook* button seen on many websites. The huge difference however is that there is no 'identity provider' or 'login provider' in the middle. Think of it like having Facebook Connect without needing Facebook.

It's all based on secure, private and direct connections between users and the application, with no other 3rd party involved. Each user relies on presenting a particular credential to complete the logon, which they have gathered and store securely in their identity wallet, the **Emerald TrustWallet.**

Turning old processes on their head

Having a trust framework where the person presenting the credentials cannot tamper with them or fake them allows us to streamline many processes, and give all parties in the value chain comfort and efficiency. Now when a person presents a digital **Emerald** credential such as:

- Copy of identity documents (passports, utility bills);
- Exam results;
- Copy of qualifications;
- Certificate of employment;
- Reference from a landlord; or
- Certificate of salary.

the recipient can see automatically who issued the original and be confident that it has not been tampered with. The credentials come in effect with a built-in seal of authenticity. We can then perform 'four simple checks':

- Who issued the data?
- Who the data was issued to?
- Whether or not it has been tampered with
- Whether or not the credential has been revoked since issue

So - no more phoning universities or employers to confirm that the documents are genuine.

Further Afield

The **Emerald** platform will be compatible with the European Union's Identity Framework eIDAS which means that credentials in your TrustWallet can be used anywhere that supports eIDAS and you see this symbol. This means that the **Emerald** network will be interoperable – by design – with similar initiatives across Europe and around the world (including Canada, USA, Finland, the Netherlands and Germany amongst many others). While eIDAS has yet to gain significant adoption in an Irish context, it is important to plan for a future where it could be the new standard, both at home and internationally.

What could the future also hold?

Travel

Imagine a future where you can travel internationally without carrying a paper passport. You may have provided a digital copy of your passport in advance to your travel agent or present that at the check-in desk for verification. You can't lose it and it can't be stolen. It would be near impossible to forge a fake passport and if a 'real' one was issued through collusion with the government agency it could be revoked on discovery.

Reference checking

We no longer need to call to check the authenticity of employment or education references: the digital credential issued, backed by the **Emerald TrustXChange**, is self-authenticating.

Health

Our medical records are one of the most sensitive and personal data sets we possess, and the transfer of which is one of the most cumbersome and least facilitated we know. How many times have we had to restate our details and circumstances, history and respective treatments in the medical sphere. In fact we could go one step further and say that a root cause of this friction is the fact that we don't self-possess our health data (supporting laws like GDPR and consent arrangements aside) – it resides in multiple systems and locations, lacking the standards and protocols for smooth transfer and chronicle.

Why would **Emerald** not be the basis for securing, storing and sharing our health history, and in time facilitate the cross referencing with family records to ascertain that all important lineage that helps detect hereditary risks. Perhaps a little far fetched, but maybe not – this is one of the great unsolved data-sharing conundrums and surely one for solving by **Emerald**, at least in part.

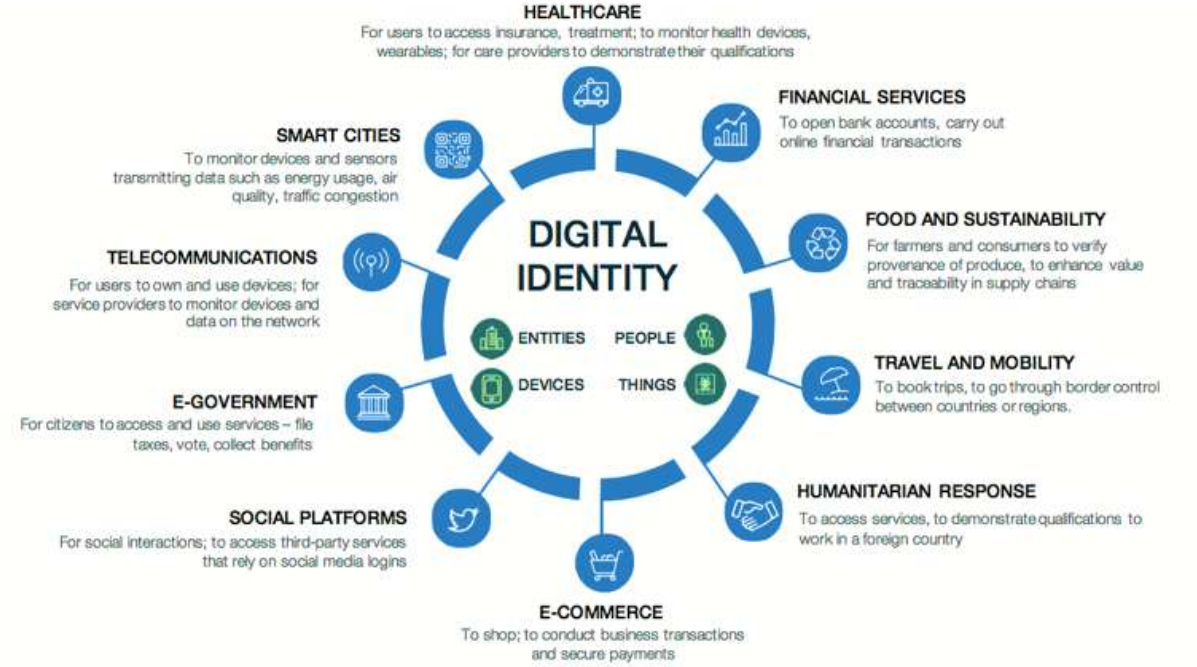
Marginalised Communities or Citizens

Emerald could, with the right level of understanding, design and enabling partners and protcols, facilitate those that are deemed to be marginalised from participating in the Digital economy benefiting from all it offers. Take for instance those that are homeless – the lack of provable address (as defined in KYC processes) and the cost associated with mainstream banking costs (to name but a few inhibitors) deters many citizens from operating bank accounts, holding debt cards, making payments, getting insurance and indeed re-entering what might be termed as mainstream, stable life.

Imagine if **Emerald** was to facilitate the creation of a profile of credentials that was strong enough meet the hurdles of identity that are required to participate in securing mainstream financial services, which today further polarises those who may already be suffering.

The Trust Panorama

What we have covered in the illustrative use cases so far only serve to unwrap and depict the broad canvas of opportunities. Identity, and the credentials that amass therein, span a broad and deep vista as illustrated below (source: WEF) and are all 'on-limits' for the purpose of our vision for **Emerald**.



How does it all work?

For a trust system like **Emerald TrustXChange** to work we need a few things :

What	Description	Examples
Credential Issuers	Organisations that will offer high quality credentials to citizens, customers and consumers In future versions, Individuals may provide proofs to each other	Typically Government, Financial Institutions, Utilities etc and other trusted institutions References for ex-tenants
Verifiers	Organisations or individuals who will accept Digital Credentials as part of one or more (business or transactional) processes	Typically everyone from individuals[2] to large organisation and Government
Credentials	Any artefact with a set of attributes signed and secured using digital signature technologies	Driving Licence, Passport, Utility Bill, Bank Statement, Degree Certificate, Tax Certificate, No Claims Bonus cert, Health Record etc. Any useful arbitrary data can be packaged as a credential
Emerald TrustWallet	A mobile phone app (iOS, Android) that support the storage and sharing of credentials	
Emerald TrustXChange Network	The platform or ecosystem that supports the secure peer-to-peer exchange of credentials between entities	

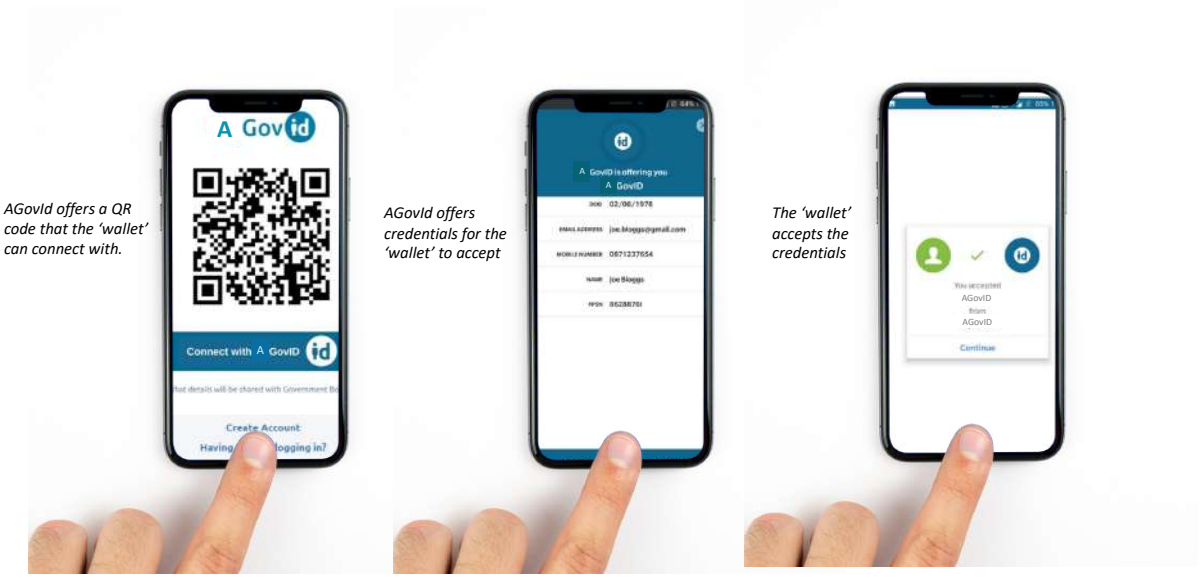
Obtaining Credentials from Identity Providers

We have been receiving credentials for centuries. We typically hold Passports, Driving Licences and receive Bank Statements and Utility Bills online or less frequently, in the post.

[2] Currently the activity of requesting a credential, known formally as a Proof Request, is only possible for Enterprises/Organisations in our demo environment. Peer-to-peer exchanges are a possible future enhancement.

Organisations participating in **Emerald** will display its logo and provide a mechanism to transfer a secure digital copy of one or more credentials to the end users **TrustWallet** to use anywhere **Emerald** credentials are accepted. Let's look at a few examples (illustration only) …

When Government agencies such as the Passport Office or Registrar of Births and Deaths issue a physical credential they can also make it available to transfer to **TrustWallet** via A GovID portal. Simply scanning a QR code from the **TrustWallet** or clicking the **Emerald** logo on their site will allow this credential to be stored.



AGovId offers a QR code that the 'wallet' can connect with.

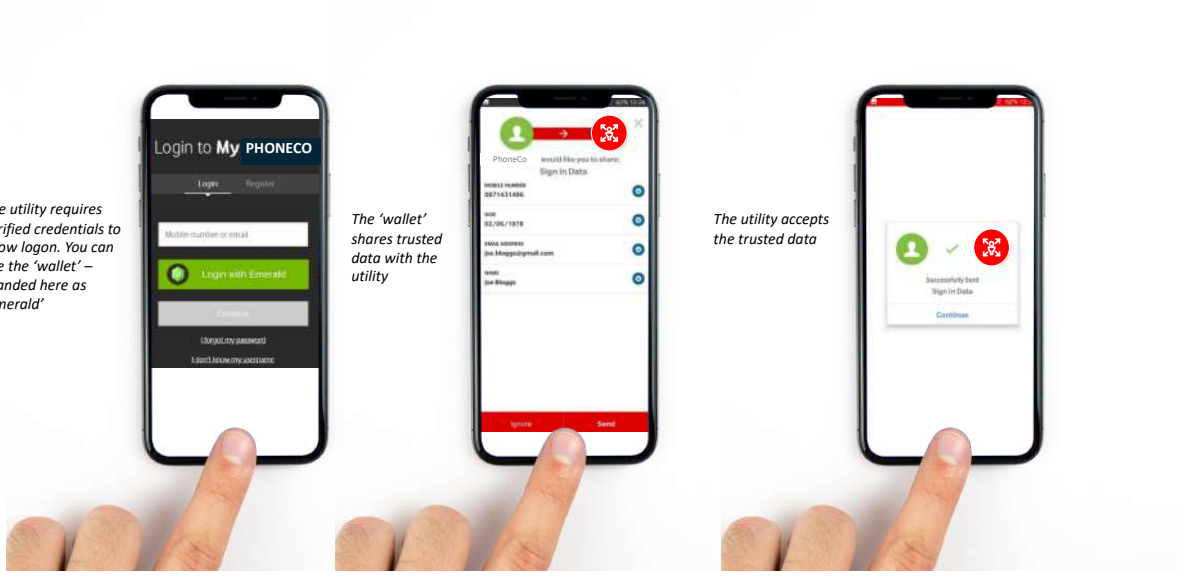
AGovId offers credentials for the 'wallet' to accept

The 'wallet' accepts the credentials

Providing Credentials to Verifiers

Once a number of digital verifiable credentials have been issued to an end user, selected attributes from any of the credentials stored in your **TrustWallet** can be provided to a third party that accepts **Emerald** credentials.

In the example below My Phoneco supports signing up and logging in with **Emerald** credential details and we use the attributes from our A GovID credential to complete the required fields. Note that we need only supply the subset of attributes required from the totality of what is available. For example a birth certificate contains many details including mother's maiden name. In the physical world a third party takes a photocopy of all of those details. In the **Emerald** world, only the essential details needed for the transaction being performed are exchanged. This is particularly powerful in the context of meeting GDPR requirements, notably data minimisation and selective disclosure.

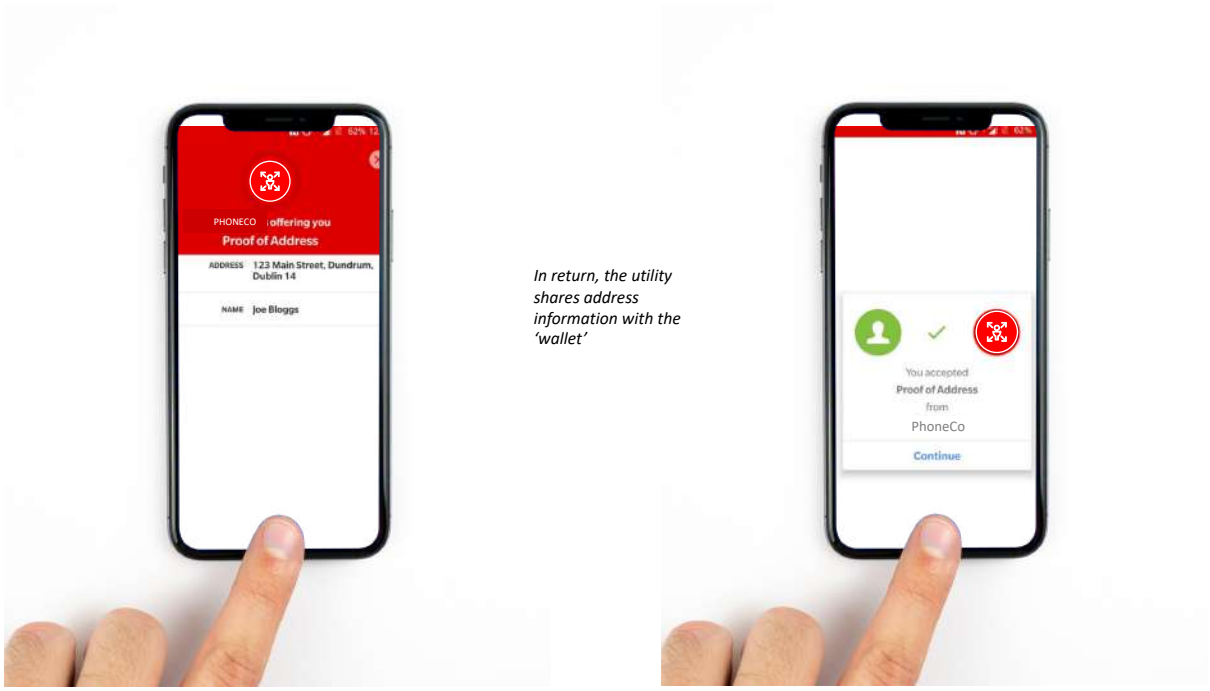


The utility requires verified credentials to allow logon. You can use the 'wallet' – branded here as 'Emerald'

The 'wallet' shares trusted data with the utility

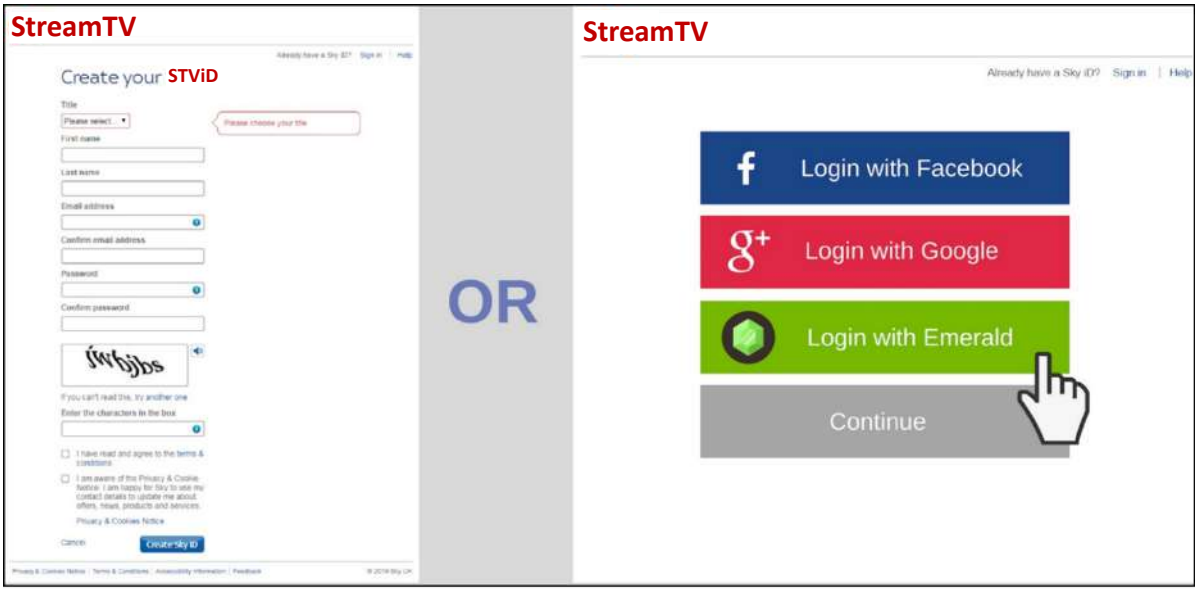
The utility accepts the trusted data

In the example above the user has signed up to My Phoneco with the **Emerald** A GovId credentials and now we are offered a My Phoneco credential with name and address (and if appropriate a confirmed mobile phone number).



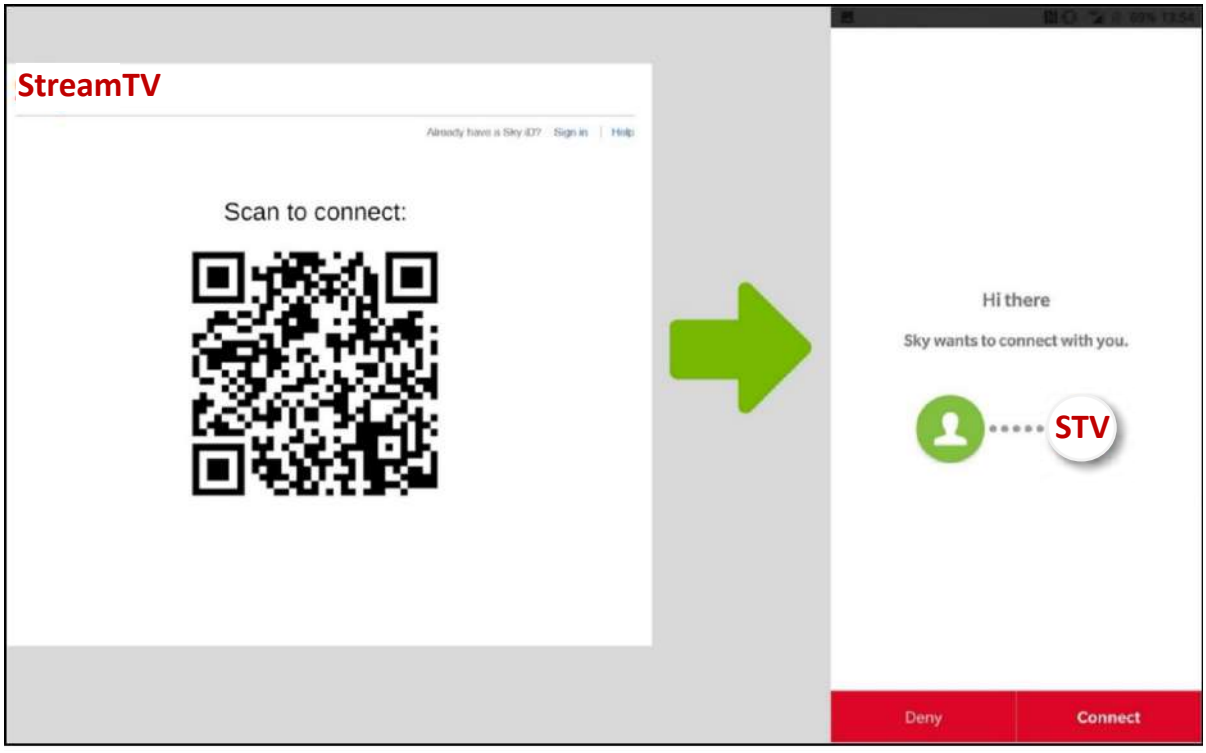
In return, the utility shares address information with the 'wallet'

Later on when the user decides to set up a StreamTV account they can do it the old way, by typing in all the details OR simply use their **Emerald** wallet.



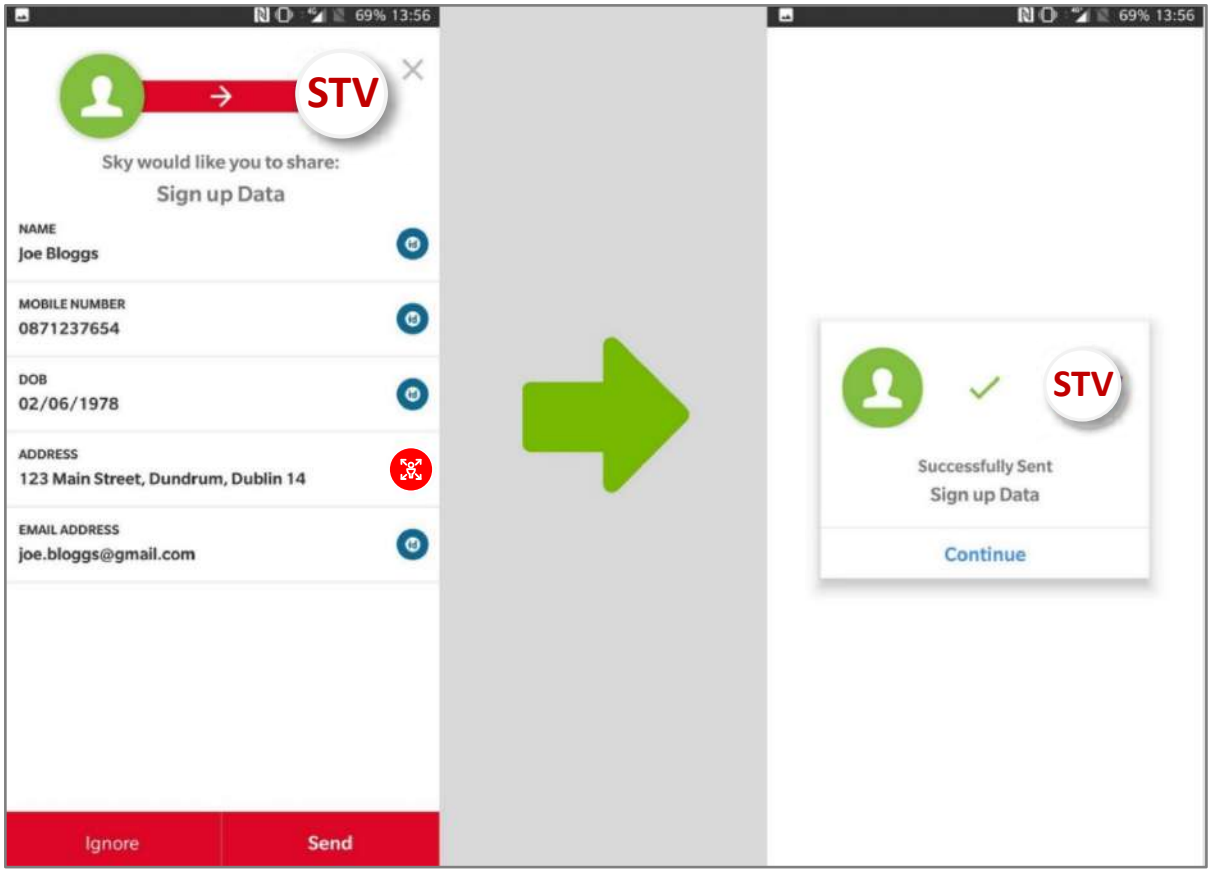
The user is now applying for a service (e.g. a tv package).
If the company supports the Emerald Wallet then the experience is transformed

In two seconds they scan a QR code to connect (or directly pass the details if using the mobile device holding their **TrustWallet**)



Scan the QR code to connect

And then they can use a combination of credential attributes from A GovID and My Phoneco (see the logos down the right hand side of the screen capture on the left below) to complete the StreamTV form without typing anything.



Frequently Asked Questions

Is this safe?

Emerald's evolution thus far is based on a globally recognised Self-Sovereign Identity Governance Framework called the Sovrin Governance Framework. This is a set of technology, legal and governance frameworks that set a high bar for protecting the credentials and identity of individuals. Credential Issuers like the Government, Financial Institutions and Utilities offer a digital credential as an option to authorised holders of those credentials. They are a digital equivalent of paper credentials that often already exist in the 'real' world.

When you choose to put them in your wallet that is the only place the digital copy exists, they aren't stored centrally. You choose when, or if, and how much of those details to share with any third parties, which is the key premise of **Self-Sovereign Identity**: your credentials, your choice.

The credentials themselves are digital certificates which use the strongest encryption technology available. When you issue them to another party they are further encrypted so that they are readable only by the person or organisation you have provided them to.

Clearly that means you need to keep your wallet safe. Like any other secure application such as online banking the **TrustWallet** can be protected by a password or/and preferably a biometric such as a fingerprint or facial affirmation. If you lose your phone it is possible to invalidate the wallet on

the device rendering it useless[3]. This means that if a person's device is lost or stolen, they only need to 'disable' that device; it can't then be used to impersonate them. The data, on its own, can't be verified unless it comes from that particular device.

Who issues Emerald credentials?

In theory, any organisation who wishes to can sign up to create and issue credentials using **Emerald**. It is an 'open' network.

In practice the most valuable or 'high-value' credentials are those issued by highly-reputable entities with strong processes in place to ensure the authenticity of the data in the credential being issued. For example the Irish Government use the SAFE (Standard Authentication Framework Environment) protocol to verify people registering for key state services. Financial Institutions are required by the Central Bank of Ireland to put in place robust Know Your Customer (KYC) processes to establish customer identity before opening bank accounts or other financial products.

A key part of the trust created by the **Emerald TrustXChange Network** is that we can verify exactly who issued the credential and that it has not been tampered with in any way.

How do I know the credential is real?

None of the personal details in the credential are stored centrally, so there is nothing useful to be stolen from a central database or registry. When someone receives an **Emerald** credential, the **Emerald** software can check the relevant ledger to confirm who this credential was issued by, that it has not been revoked and locally verify the digital signature accompanying the credential to confirm that the contents have not been tampered with.

While a detailed explanation of Blockchain is beyond the scope of this document, the core design principles of Blockchain mean that this store of verification information is not owned or controlled by any single party; we actually use the Sovrin Network which is hosted and managed by over 70 independent high-quality Sovrin Stewards who participate in ensuring the integrity and tamper-proof nature of that data. These range from IBM and Cisco, to NEC and ABSA (Barclays Africa).

What happens if my credential is stolen?

The credentials in your wallet are encrypted with secrets known only to you, and in many cases a biometric such as a fingerprint which makes it difficult or impossible for a third party to break them.

If you provide them to a third-party the copy is in turn encrypted in a way that it can only be read with their secret code – so even if the third-parties copy is intercepted it can't be read by another. These protections don't exist for a photocopy of a physical document. Also the credential can be marked with details of who it has been provided to and for what purpose so even if you share a copy

[3] This is a roadmapped feature, not currently available.

of your passport with me for a purpose, I couldn't use the copy you provided to me and provide it to another third-party as my own passport.

Why is this happening in Ireland?

There is global interest in secure Digital Identity and Credential exchange systems. By creating **Emerald** in Ireland we can make business and life easier in our country and integrate with or adapt global solutions and standards when they gain widespread adoption.

A number of years ago Irish Banks introduced the Laser Debit card standard to allow debit card transactions to take place in the country. This was retired once the globally accepted VISADebit standard was widely adopted and Laser was superceded by it.

We may see a similar trend with **Emerald** in due course. The opportunity here is to accelerate identity innovation in Ireland, and become a leading digital nation to enjoy the citizen, social and economic benefits that brings.

Who or what is Emerald?

Emerald TrustXChange is a not-for-profit limited company[4] founded by a consortium of public and private sector companies to advance secure, self-sovereign identity and credential sharing for the island of Ireland. Initially championed by Irish Life, the insurance company, the consortium rapidly grew to include the Irish Government and host of blue-chip organisations.

It is to exist as a public good, governed by a Trust Document and charter, and managed by a Board of Trustees for the benefit of all. Seen as a utility to serve a public good, companies and individuals can gain efficiencies and make profits through leveraging the **Emerald** capabilities.

Emerald itself does not exist to make a profit and promotes universal access to those with a legitimate interest in activity taking place on or with citizens of the island of Ireland. While that is the broad focus we are also keen to support inter-operability with international digital identify schemes as that becomes feasible and appropriate. At all times the right of the individual to choose whether to participate is sacrosanct.

Where to next?

The purpose of this paper is to briefly set out the challenge of Digital Identity, and mostly to paint a picture of the panorama of benefits that a national solution like **Emerald TrustXChange Network** could of fer. Many enabling and success considerations spanning proposition and brand, the prioritisation of use cases, technology, operations, governance, data stewardship, liability, policy and legal frameworks, funding model and monetisation opportunity structures (to name but a few) need to be posed and solved.

[4] The actual legal structure of Emerald TrustXChange is yet to be finalised.

Those are for another day, and other documents which are in development in parallel. For now the **Emerald Team** wish to share their vision for what could be, and how it could be. We welcome and invite all and every participant to join us in making what is rational, desirable and auspicious a reality.

Curious parties, specialist advisors, fully-integrated Identity Providers or Verifiers and anyone looking to find out more or make a contribution can find more details at our LinkedIn Group https://www.linkedin.com/groups/8912523/

We look forward to hearing from you

References

	World Economic Forum Blueprint for Digital Identity http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
	McKinsey Digital identification: A key to inclusive growth https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
	Comprehensive Guide to SAFE Registration and the PSC https://www.welfare.ie/en/downloads/DEASP_Comprehensive_Guide_to_SAFE_Registration_and_the_PSC.pdf
	Blockchain definition - Wikipedia https://en.wikipedia.org/wiki/Blockchain
	Deloitte Picture Perfect: A Blueprint for Digital Identity https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-digital-identity-online.pdf
	BBVA Digital Identity: The current state of affairs https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf
	Sovrin Document Library https://sovrin.org/library/
	EU Electronic Identification, Authentication and Trust Services https://en.wikipedia.org/wiki/EIDAS