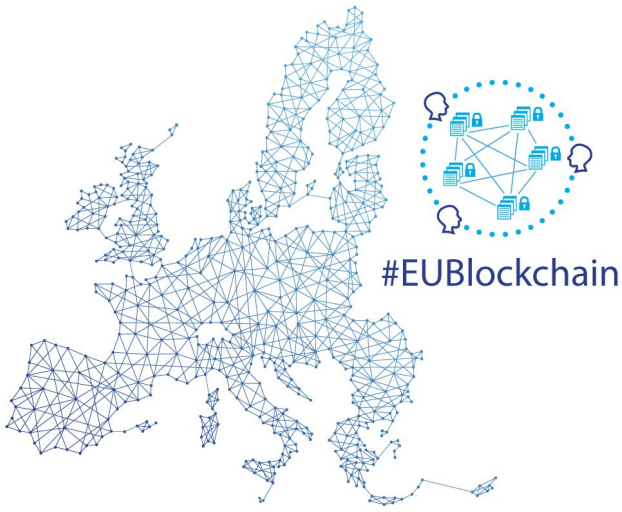
EU Blockchain Observatory and Forum

An initiative of the European Commission

EU BLOCKCHAIN OBSERVATORY AND FORUM

Workshop Report
e-Identity, Brussels, November 7, 2018



By the European Commission, Directorate-General of Communications Networks, Content & Technology.

Author: Jérémie Grandsenne
Published on 27 November, 2018
Comments and inquiries may be addressed to the following email: info@eublockchainforum.eu

Table of Contents

Opening and introduction

The workshop was opened by Pēteris Zigalvis – Head of Unit, Digital Innovation and Blockchain, Digital Single Market Directorate, DG CONNECT.

The workshop was then introduced by Ludovic Courcelas, European Union Blockchain Observatory & Forum, defining the objectives of the day:

- Define what the decentralized identity framework looks like and the industry standards used
- Explore how to integrate that framework with eIDAS
- Clarify the use of blockchains for decentralized identities
- Define the infrastructure and regulatory requirements for a European blockchain infrastructure identity module

Presentation – Andrea Servida; Carlos Gómez Muñoz: The eIDAS regulation, and how it may be linked to blockchain

Andrea Servida - Head of Unit "eGovernment and Trust", DG CNECT
Carlos Gómez Muñoz - Policy Officer – Seconded National Expert, DG CNECT

1) eIDAS

• What is eIDAS
- eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation and a set of standards for electronic identification and trust services, for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification.
- eIDAS notably contains:
Chapter II: Mutual recognition of e-identification means
Chapter III: Electronic trust services: using electronic identification means using services provided by public services.
Chapter IV: Legislation on electronic documents: An electronic document can not be rejected by the court for the reason that it is electronic.
- eIDAS defines what legal proof a cross-border transaction may carry.
An electronic signature carries the proof of origin, the exchanged content, timestamp, and requires the identification of the sender and of the recipient, and the confidentiality of the

exchange. Timestamp is a way to prove that what the sender claims to have sent is what has actually been received.

• eIDAS: Key Principles for Identity

- Key principles are:
    - Cooperation between Member States
    - Principle of reciprocity relying on defined levels of assurance
    - Mandatory cross-border mutual recognition between Member States to access public services, meaning that identificators delivered by one Member State can be used and recognized in another Member State.
    - Sovereignty of Member states to use or introduce means for eID at their national level, meaning that there is no constraint at the European level to rule the way in which identity should be harmonized.
    - Full autonomy to the private sector
    - Interoperability framework
- Member States can use different means of identification, but with the same functionality: trustworthiness of the credentials attached to the means that are used. If one uses a citizen card in Austria to access a governmental service, she will be able to use this same card to access services in Sweden.
- The problem is not the technology, but the legal framework, the distribution of liability, and the question to know whether what is enforceable in country A is also enforceable in country B (for instance in the court).

• The eID ecosystem

- Member States operate Nodes, that are linked to identity attributes providers. Citizens can use these attributes with Service Providers (entities providing services using ID), both in their country and in other Member States' public services.
- The citizens can use the services in a way that proves that the attribute they are providing is linked to an identity, without providing the whole of this identity, only the needed credentials for a specific purpose: the goal is that the identity speaks for us, and not about us.

• The benefits of interoperable and recognized eID for the different actors

- Citizen (uses ID): Ease of use, cost saving, increased assurance, increased privacy, portability: for instance, I can ask my bank in my own country to move the credentials (KYC) needed by another bank in another country.
- Public administration (set up): Cost saving, compliance, increase assurance
- Identity / Attribute providers (provide identity and attributes): New areas of application
- Service providers (offer services using ID): Cost saving, legal compliance, Increased security and assurance, Increase potential user base

• eIDAS: Trust services

- Electronic signatures, including validation and preservation services
- Electronic seals, including validation and preservation services

- Time stamping
- Electronic registered delivery service
- Website authentication

2) How is eIDAS Implemented

• **eID Components and Interoperability**
- When a citizen from a Country A wants to use an online service provided by an authority in a Country B, this falls under the scope of the eIDAS regulation, in the electronic identification part.
- This is done through the nodes, that create the trust framework, and through eIDAS' interoperability framework: eIDAS nodes in country 1 are linked to identity providers and to identity attributes providers, but also to eIDAS nodes in country 2, so that the information can be shared if needed, and attributes issued in country 1 can also be used in country 2.
- An eIDAS-Node is an implementation of the eID eIDAS Profile, able to communicate with other nodes of the eIDAS Network. An eIDAS-Node can either request (via an eIDAS-Node Connector) or provide (via an eIDAS-Node Proxy Service) cross-border authentication.

• **Minimum Data Set**
- Citizens' information divide into mandatory / optional / sector specific attributes.
Mandatory information include: current family name(s), current first name(s), date of birth, and a unique identifier as persistent as possible. Examples of optional information: address, gender. Examples of sector specific: social security number, tax number.
- There is no anonymity.

• Types of e-Signatures and e-Seals
- Technically, e-signature and e-seal are the same, but the legislation makes a difference between a natural person's sign, and a legal person's seal. Legal person's information also divide into mandatory / optional / sector specific.
- Simple / advanced / qualified signatures:
Simple Electronic Signature (SES):

- Demonstrates the intent of the signer
- Associated with the document or data the signer intends to sign or seal

Advanced Electronic Signature, AES, simple electronic signature which also:

- Identifies, is uniquely linked to and under the sole control of the signer / sealers
- Detects subsequent changes to the document
- For mutual recognition by public services, must be in ETSI formats (ASiC, PAdES, CAdES, XAdES)

Qualified Electronic Signature, QES, advanced electronic signature which also:

- Is based on a qualified certificate
- Is created using a qualified signature creation device
- Equivalent to handwritten signature

• e-Signature and e-Seal Creation Tools

Multiple signing options are available: local (PC) / mobile (phone) / remote (cloud), all acceptable. What matters is what is required for each of the below options:

- Required for SES:
    - A user electronic identification (eID) means
    - An application managing the signature / seal creation process (to enter the PIN, to select the certificate)
- Required for AES:
    - Digital Certificate issued by a national Certificate Authority
    - Qualified Digital Certificate issued by a Qualified Trust Service Provider
- Required for QES:
    - Qualified Signature / Seal Creation Device

This is the minimum, but the service providers can add any supplementary kinds of identifiers to prove that the person's identity is linked to these identifiers.

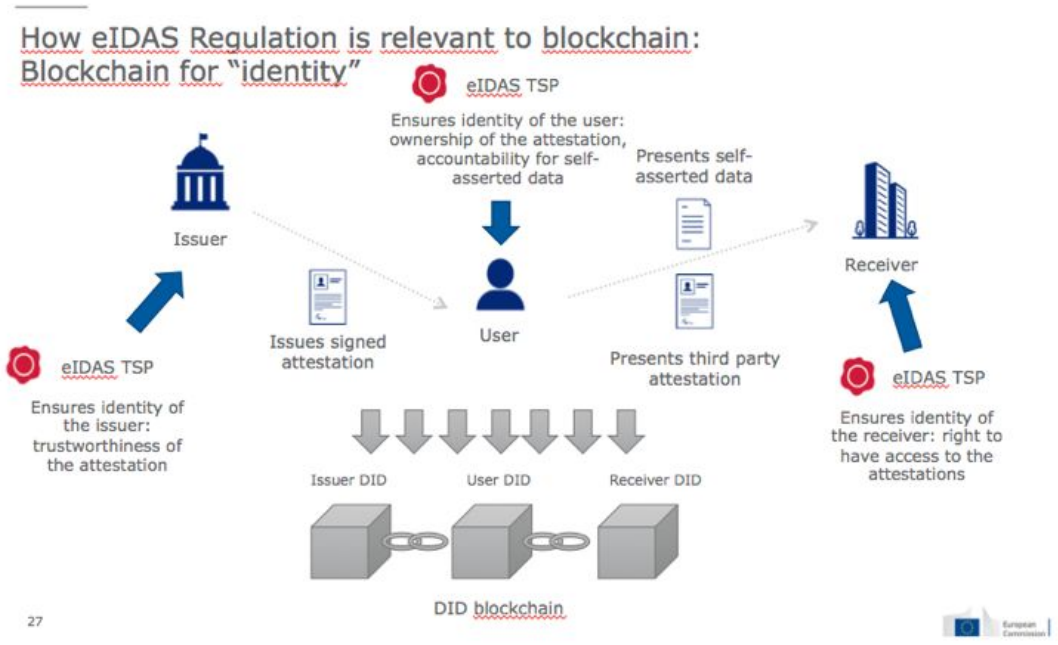
• eIDAS and Blockchain: Inserting Content on the Blockchain

- The content of the blockchain is an electronic document:

Blockchain is basically data and hash. Under the eIDAS regulation, blockchain's data, stored in blocks, is an « electronic document », as « electronic document » is defined by the eIDAS regulation as any content stored in electronic form (article 35).

- As soon as you put some content as electronic document, you are under the eIDAS regulation: you don't need to be « eIDAS compliant », you are already under eIDAS. And if a content is signed, it is under eIDAS, however you sign it.

• eIDAS and Blockchain: Blockchain for « identity »



TSP: Trust Service Provider

- If blockchain uses digital identity, the eIDAS regulation creates a framework that creates trust in that identity. You can implement whatever you want related to digital identity, but if you rely on the eIDAS, you create the certainty that is provided by the eIDAS, especially for sectors where the legal identity may play a role: travels, finance, payments…
- Role of the Trust Service Provider: The receiver needs to know that the information he's receiving is really issued by the appropriate source. The role of the Trust Service Provider is precisely to link the real identity to the digital identity, by means of electronic certificates.
- eIDAS provides the platform thanks to which services that need the true identity can rely on it, and in a way that is privacy-protected: for instance, to open a bank account, there can be a KYC available on the blockchain that doesn't reveal the person's true identity.

Panel discussion – e-Identity Standardisation: State of the Art

This panel was moderated by Susan Poole. The panelists were:
Carlos Pastor - Alastria
Oliver Terbu - uPort
Luca Boldrin - Infocert
Patrick Curry - BBFA
Ronny Bjones - Microsoft
Kai Wagner - Jolocom
Ken Timsit - ConsenSys

Highlights of the discussion included:

1) Concepts and Context

• Authentication and Privacy
- Mutual authentication: service provider and user authentify each other in both directions.
- Privacy: Unlinkable actions. Authentication should be unlinkable for third parties: when I present a claim to a service provider, nobody will know that I present this claim to this service provider.

• Paradigm shift: user-centric private data management
- Until today, big corporates pick up the data. We should put the data in personal stores, in an encrypted way, so that all aspects of our identity will be linked in these personal stores. We

have to do it in a very seamless and intuitive way, both for users (citizens) and for developers (developing applications and services based on this new paradigm).
- Users can now create their own decentralized identities, put them on the blockchain, and they can always go back, to prove that they are the owners of that specific identities.

• 3 approaches for the chain of trust
- Classically bind: a government issues an identity to a citizen, which is then used in a chain of trust by reliable parties to issue further credentials, which are used in society.
- Late bind model: Self-Sovereign Identity (SSI). You start with a token or a cryptographic primitive, and you bind attributes to it for use. The problem with that model is low assurance, and the fact that SSI is an intermediary in the trust chain.
- Third model: The relying party and the user are directly validating against the authoritative source. There is no intermediary, no token, and this is a high-assurance environment. The World Economic Forum is looking for that, especially for border-control.

• eIDAS versus Self-Sovereign Identity (SSI)
- The eIDAS world provides strongly validated identities.
- SSI offers lower assurance, but offers support for a large set of providers. There are many ways to introduce a secondary identity next to your primary identity that is the national one, and SSI would be the most viable way to add it.

• Decentralized identifiers - DIDs
- Technically, strings of characters
- Registered on a blockchain or a decentralized network
- Ledger agnostic, interoperable
- Based on the DIDs, you can resolve a DID document, that contains a set of cryptographic material, like a set of public keys, and also service endpoints.
- You can use these keys to do anything: authenticate the user, verify digital signatures generated by the user, have end-to-end communication with the user…
- DIDs are the foundation for many decentralized platforms.

2) Existing standards

• **Open ID Foundation**'s standard **Open ID Connect** is used by many applications, using JSON as a data format (JSON is for JavaScript Object Notation, a very commonly used data format).
- Model: Many security primitives have been defined, electronic signatures have been put on them and encrypted, and they have all been plugged into this standard.
- Open ID Connect is currently clearly the more widely used standard.

• **W3C**'s **Verifiable Credentials**, and W3C **Decentralized Identifiers (DIDs)**
These Verifiable Credentials are currently working on a data representation that allows easier exchange of these credentials between different entities in the decentralized ecosystem.

• The **Decentralized Identity Foundation** is dealing with concepts like Identity Hubs and Decentralized Data Stores

• A lot of work has been done by the **IETF**, Internet Engineering Task Force.
The IETF is an open standards organisation, developing and promoting voluntary Internet standards, especially the standards that comprise the Internet protocol suite TCP/IP.

3) Current interoperability of Identity solutions

• Several interoperabilities to rule them all
Interoperability in e-Identity doesn't mean one but several interoperabilities all together, particularly for assurance purposes: data interoperability, cryptographic interoperability, system interoperability, technological interoperability, and policy interoperability, which is the hardest part. eIDAS has faced most of it, but maybe not all of it. The higher the expected assurance level, the stronger these interoperability mechanisms have to be.
So then for instance, you can have a SAML protocol in the back-end, and in the front-end an Open ID Connect protocol, both interfaced with each other. (SAML, Security Assertion Markup Language, is an open standard for exchanging authentication and authorization data between parties, in particular between an identity provider and a service provider.)

• The trust framework
What is really relevant for the business, is an identity that implies a liability behind, and eIDAS brings this liability.
Other schemas are possible with a lower liability, or that require to build up a liability schema behind, which is costly. Hence, it's more convenient to import a liability schema directly coming from the eIDAS trust framework.
- While SSI is focusing primarily on *authentication*, it is not engaged in identity *proofing*, which is the core activity to prove that someone is who they claim to be. For instance with eIDAS, we're trusting the governments to have a strong identity proofing process, so that we know for sure who someone is and is not. How credentials are issued, that then got used and consumed in SSI, really needs to be understood, otherwise relying parties will not trust the relying solutions.
- While SSI solutions don't really solve the issue about trusting the issuer of the attestations, these standards that are currently under development, like Verifiable Credentials and DIDs, allow to integrate trust frameworks, and allow issuers to be trusted through the ecosystem. So eIDAS may be a great opportunity to leverage SSI solutions.

4) Using blockchain for e-identity standardization

• What (not) to store on the Blockchain

- Blockchain is the association between a public key and an identifier. It can be used for Decentralized Private Key Infrastructure, DPKI, which is the core.
- Data or content can be stored on the blockchain, but it's not necessarily the best way to do it, and personal data must not be stored on the blockchain, because of the GDPR.
- The blockchain doesn't necessarily have to store the credentials themselves.
- There is nothing that needs to be stored on the blockchain, a DID should simply be anchored there: for instance, an Ethereum address is generated, and because it's an Ethereum address, everybody knows how to resolve the public key based on a signed message. Then, the message can be verified without going to the blockchain.

• The benefit of using the blockchain for e-identity
- You need to be able to see that somebody is bringing an identity or an identifier from some source, and to identify that directly from that source. What blockchain offers for the identity space, is that it allows you to provide identity without having to rely on one central source of trust, or one central registry.
- You can have several registries working together interoperably because of the way of establishing identifiers, and because of the way of registering them and making them resolvable.

• How to integrate both eIDAS and the blockchain to an identity framework
- eIDAS is a necessity, because regulatory reasons require to stay strict on the primary identity.
- But a blockchain-based approach can be leveraged to create secondary identities, as there is a strong request from the commercial world to benefit this trusted data.
- Being able to reuse nationally proved identification material is a huge benefit, both for public administrations (time saving), and for businesses wanting to use these information.
- Using eIDAS, and additionally blockchain or SSI, allows more trustworthy credentials from eIDAS identification means, or allows to leverage Trust Service Providers, e-signatures, or even qualified signatures, to provide qualified attestations when needed.
- A clear interface is crucial, otherwise people won't use it. We should go for solutions that truly allow the user or the entity that is involved to handle everything from one interface.

5) Timeframe for these standards to become a reality in our daily lives

• Some standards are already adopted even if people don't know it
- For instance, ISO/IEC 29115, the Entity Authentication Assurance Framework EAAF, https://www.iso.org/standard/45138.html,
which includes the identity proofing stage, the credentialing stage, and the authentication stages. It is already implemented in many areas of business, especially aerospace and defense, and supports a lot of processes in airlines today.

In Estonia, privacy management for all citizens is done on that basis, as well as ID cards, and many other ID cards systems in Europe are also based on it.
- There are lot of standards, the question is how to educate people.

• Timeframe for the standardization of identities in the blockchain ecosystem
- There are already many ISO standards, because identity has been standardized for many years. The challenge for the blockchain standards is to be a unifying force, to combine those standards inside a framework.
This work is already in progress: the W3C standards on Verifiable Credentials will come Q1 2019, and DID specifications are already version 1.0.
- Not many eIDAS compliant SSI projects are already in production, but there's work ongoing for it. There is a list of pilot implementations at the end of the Bundesblock SSI position paper.
- There are other identity solutions using blockchain, not relying on the SSI model.

Working sessions – What are the necessary standards to implement e-identity in a european context? European blockchain infrastructure: regulatory and infrastructure requirements for e-identity

The talks have allowed to highlight the following points:

• Actors of the model
- Subject: citizen
- Verifier: entity trying to verify something and get some info about the subject's identity
- Credential issuer / Trust anchor
- Blockchain
- User agent (for example: mobile application, PC software), meaning frontend (interface) + Identity Hub (credentials storage space)

• Model
- A credential issuer (Service Provider) issues a Verifiable Credential X, that is stored in an Identity Hub.
- The subject is connected to a website owned by the government, and needs this Verifiable Credential X to perform a certain action or make a certain request to the government.
- The subject does a request to the verifier to get her Verifiable Credential X.
- The verifier (Service Provider) sends a request to the user agent (application)

- The verifier can now issue a credential to the subject, for the subject to use it wherever she needs

• Structure of the DIDs and Verifiable Credentials Ecosystems
- DID Attestations come with:
Decentralized identifiers (DIF)
DIF Identity Hub, to store the attestations one owns
DIF Universal Resolver, a registry acting as a correspondence table between credentials and addresses
- Verifiable Credentials (W3C):
Every decentralized ID will be stored in the Verifier Registry
- DID attestations and Verifiable Credential are basically two words for one thing. But there is a difference between DID Revocation and Verifiable Credential revocation: DID is only a public / private key relationship, while Verifiable Credential is about my credential issuer that would be able to revoke my attestation at some time.

• Who hosts the space to store the data of the DIF Identity Hub ? / Who operates identity hubs ?
- At the moment, Microsoft uses an identity hub on the device. In principle, the identity hub could be simply a binary piece of encrypted data.
- Identity hubs could be operated by many providers, all in competition, and each user would select the one she uses, like she choses an internet provider.
- They can also be on one's own computer, connected to the internet.
- It is not necessary to have the Identity Hub on the blockchain, and it is very complicate.

• 2 distinct questions when thinking about ID and blockchain
- Understanding the process of someone identifying himself and making statements using a smart contract, and making a claim to a blockchain address
- Examining blockchain as a tool that helps making those claims easier

• **Benefits and implications of storing the Verifiable Credentials on the Blockchain**
- The Verifiable Credential is timestamped, making you both able to prove when it was issued, and unable to fraud about its issuing date.
- You can share the verification for the same attribute, example a KYC for banks, once for all. (Although right now, we have no proof that a bank B will accept a KYC used by bank A.)
Counterpoint: it's hard to control who has access to knowing that there is a Verifiable Credential here or there.
- Notarized credentials are hashed personal data, and might be or not be considered personal data by GDPR, and so might be or not be allowed to be on the blockchain.
The linkability risk means identifying pattern, comparing infos, and deducing a hash / ID association, and this risk makes it preferable to look at one time hashes that can't be analyzed.

There is also a reversibility risk, which means finding the original input from the hashed output, and currently there is no law case on this point. Still, nonces added to hashes might prevent reverse identification.
- Verifiable Credentials requests (for the Verifier to retrieve the credential in the Identity Hub) enclose the Verifier's DID, and currently there is no standard, such as the JSON format, for this request.
- Step 1 is the user online request. The user needs to be recognized, but she also needs to be sure that she is identifying for the real website: to check this, she uses the DIDs registry. Setting a registry at the EU level might be a good initiative.
- For the online request process, the user's browser is redirected to the Verifier, and then the user does the action of identifying himself. The call is sent back to the user agent (application), and retrieves the verifiable claim. The verifier will have an agent acting on his behalf, so there are initiatives to standardize this agent-to-agent communication, but still none is used as a *de facto* standard.
Microsoft, uPort and others are building user agents, but each has its own methodology and documentation to get through if one wants to interact with it.

• Private keys and Value of the credential
- Natural persons are able to create and register their private keys. But when I want to act as an issuer, comes the question of what my private key is, and whether I can be trusted.
- Qualified public or private organisations are supervised, and the registry of certificates is public, which allows to check that the document was actually sealed by who is claimed to have sealed it.

Pēteris Zigalvis presented during the session the ongoing European Blockchain Services Infrastructure (EBSI) initiative, stressing the following elements:
• European blockchain infrastructure
- We should have the functional and technical specifications by the end of the year.
- One infrastructure versus several infrastructures coming together: There will probably be applications layers running on top of existing protocols.
- The further goal for the next seven years will be to have a permissioned but decentralized blockchain, used for the public services (a public permissionned network can mean for example that only governments can write on it).
And for a further future, to have APIs, interoperability…

• Actions required to accelerate the adoption of e-identity within the EU
- Integrating that framework with eIDAS
- Incentivizing governmental entities to issue Verifiable Claims. Ways need to be found for this: for instance, a way to monetize the issuance of credentials. Companies could save a lot of money by speeding up the process, so there is a lot of value associated with those credentials, and this value can be monetized. And the financial argument is very easy to make, because KYC is very expensive.

- The associated question is where lies the liability of the issued attestation: if it is on the company, there is a risk of refusal. If it's on the user, it will be easier for the companies to accept.
- In some countries, governmental entities must pay to access certain data. We need to move to the idea that the data belongs to the citizen, not to the government.

Appendix

Workshop slides

- Full day presentation
- eIDAS presentation
- Panelists presentations

Workshop videos

- Videos from this and all other workshops can be found on the EU Observatory website under reports
- Videos specific to this workshop:
    - Part 1 Introductions
    - Part 2 eIDAS and blockchain
    - Part 3 Panel discussion
    - Part 4 Working sessions

Agenda

Time	Duration	Activity
9:30	30min	**Guests' reception**
10:00	15min	**Introduction of the day - Agenda and objectives of the day**
10:15	40min	**Presentation - DG CONNECT, eIDAS regulation and how it may be linked to blockchain** Andrea Servida - Head of Unit "eGovernment and Trust" Carlos Gómez Muñoz - Policy Officer – Seconded National Expert
10:55	1h35	**Panel discussion - e-identity standardisation: state of the art** Carlos Pastor - Alastria Oliver Terbu - uPort Luca Boldrin - Infocert Patrick Curry - BBFA Ronny Bjones - Microsoft Kai Wagner - Jolocom Ken Timsit - ConsenSys
12:30-13:30 Lunch break		
13:30	1h15	**Working session - What are the necessary standards to implement e-identity in a european context? User journey and use cases**

14h45	1h15	**Working session - European blockchain infrastructure: regulatory and infrastructure requirements for e-identity**
16:00	15min	**Conclusion**
16:15		End of the day