INATBA
Identity Working Group

Response to the EU Commission Open Public Consultation on the eIDAS Regulatory Framework

International Association for Trusted Blockchain Applications

2 OCTOBER 2020

Avenue de Tervueren 188A/4, 1150 Bruxelles - Belgium

2nd October 2020

Re: INATBA submission to DG CONNECT open market consultation on the EU Commission Open Public Consultation on the eIDAS Regulatory Framework

Dear Sir or Madam,

Please find enclosed INATBA's submission which has also been submitted through the web portal.

This letter and submission serves to highlight and summarise the varied opinions of our membership base.

Our relatively young and highly innovative industry represents a significant opportunity for the European Commission to facilitate the establishment of Europe as a leading global location for blockchain and distributed ledger technologies.

The submission has been drafted by members of our digital identity working group, representing a diverse set of experienced and innovative individuals and their respective organizations. Identifying the upcoming process of eIDAS evaluation as a critical development for our industry, we are looking forward to seeing this process continue and will be happy to engage in and support all upcoming steps in this process.

The project was led by the Co-chairs of the INATBA Identity Working Group Kai Wagner & Alex Puig.

INATBA Executive Director **Marc Taverner**

International Association for Trusted Blockchain Applications

Association internationale sans but lucratif

Avenue De Tervueren 188A 1150 Bruxelles
Belgium

www.inatba.org

Registration number: BCE 0725685704

Bank details: International Association for Trusted Blockchain Applications

Volksbank Mittweida eG Markt 25, 09648 Mittweida

IBAN: DE 5587 0961 2401 9714 8560
SWIFT-Code: GENODEF1MIW

Table of contents

Brussels, 2 October 2020

1. Introduction

Digital identity enables transactions in the digital world. In a hyper connected world, the ability to establish individual identities of natural persons, legal entities, machines and devices uniquely, accurately, quickly and securely is going to be critical and has a considerable potential for wealth creation.

The COVID-19 crisis clearly demonstrates the need to provide all European citizens and businesses quickly with a universally accepted, trusted digital identity and with trust services such as eSignatures to allow for seamless business continuity in the Single Market and to access to crucial and sensitive public online services such as in eHealth, eGovernment or eJustice. Universally accepted trusted identification and authentication enables effective protection of personal data in the online world. At the same time, it promotes business cases based on a discretionary disclosure of data and creates the conditions for a responsible and accountable management of data and artificial intelligence in society. Using these opportunities contributes to the recovery of the European economy and to the European digital autonomy. The revision of the eIDAS Regulation is therefore part of the Commission's response to the crisis.

With the adoption of the eIDAS Regulation in 2014, the EU broke new ground globally by introducing a first cross-border framework for trusted digital identities and the so-called trust services such as electronic signatures that can be used to sign documents in the online world, much like one signs a document with a pen in the offline world. The eIDAS Regulation is meant to ensure secure and seamless electronic interaction between citizens, businesses and public authorities. This should increase trust in the internal market and make online services more effective. The European Commission is currently evaluating this regulatory framework .

The eIDAS Regulation ensures:

- that individuals and businesses can use their own national electronic identification schemes (eIDs) to authenticate when accessing public online services in other EU Member States. This is achieved by establishing an interoperability framework and by enforcing mutual legal recognition of notified schemes;
- the development of a European internal market for electronic Trust Services (electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication) recognised across borders with the same legal status as traditional paper based processes.

The Commission will assess to what extent the eIDAS framework remains fit for purpose, i.e., to deliver the intended outcomes, results and impacts and whether it is appropriate to modify the scope of the Regulation or its specific provisions, taking into account the experience gained in the application, as well as technological, market and legal developments.

In its Communication on Shaping Europe's Digital Future, published on 19th February 2020, the Commission took the position that universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them. The Commission will consider revising the eIDAS Regulation to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

The aim of this public consultation is to collect feedback on drivers and barriers to the development and uptake of eID and trust services in Europe and on the impacts of the options for delivering an EU digital identity. It targets broad public (e.g. citizens and end-users, including older persons and persons with disabilities) as well as companies directly impacted by the eIDAS Regulation (e.g. trust service providers, identity providers), competent authorities in the Member States, international organisations and concerned stakeholders on the eIDAS framework.

2. About you section skipped for INATBA members

3. General questions about electronic identification (eID)

Individuals and businesses can use under eIDAS their own national electronic identification schemes (eIDs) (e.g. government issued eID cards/Apps) to authenticate when accessing public online services in other EU Member States. This is achieved by establishing interoperability of different national eIDs and enforcing mutual legal recognition of notified schemes.

In the context of this consultation, an eID is a means of electronic identification (it ascertains "who you are") and authentication (it proves that "you are who you say you are") issued by an organisation to be used in a wide range of online services provided by different organisations. A national identity card that can be used in eGovernment services provided by several agencies, or a social network login account that you can use in several online shops would qualify as eIDs, but the credentials given to you by your bank to access exclusively their online banking services would not.

Do you have an electronic identification means (eID) which can be used to access online services?

Yes
No
Don't Know

What type(s) of eID do you use? (multiple choice allowed)

eIDs provided by my government or other public authority
Personal user accounts provided by social networks or online platforms
eIDs provided by other private sector organisations (e.g. trust service providers, banks, mobile operators)
Other

If other please specify:

The majority of INATBA members use eIDs provided by governments or other public authorities. However, others use personal user accounts provided by social networks or online platforms and some use eIDs provided by other private sector organisations.

How often do you use your eID to access or use online services?

Everyday
Once or twice a week
Once a month
Less than once a month
Never
I don't know / no opinion

For what services do you use or would you like to use your eID?

	I already use my eID	I would like to use my eID
Public services (e.g. fill in your tax form, request certificates, …)	**X**	1
Utility services (energy, water supply), telecom services		**X**
Medical (eHealth) services		**X**
Open a bank account		**X**
Shop online		**X**
Access online platforms (e.g. social networks, my online streaming account)	**X**	
Other		

***Have you found the availability of the eID means or the electronic trust services (e.g. electronic signature) particularly useful during the lockdown measures introduced due to the COVID-19 crisis?**

Yes
No

If Other, please specify:

If no, what was the reason? (multiple options can be selected)

I do not have them or could not get one (e.g. face to face interaction was needed to obtain/activate/renew an eID/eSignature certificate during the lockdown)

The online services I would need to use are not available for my eID / eSignature tools

I could not access the online services I would need due to usability / technical issues (e.g. lack of a card reader, software incompatibility, accessibility barriers for persons with disabilities)

Lack of trust

Other

If Other, please specify:

The eIDAS Regulation ensures that individuals and businesses can use their own national electronic identification schemes (eIDs) to authenticate when accessing public online services in other EU Member States. This is achieved by establishing interoperability and enforcing mutual legal recognition of the so called notified schemes. The list of notified national eID schemes is published here.

Are you aware that you can use one of the notified national eID schemes to access online public services in other EU Member States?

Yes

No

If you have one of these notified eIDs - have you ever used it to access online services in another EU Member State than your country of residence?

Yes

No

Maybe

How important for you is the ability to use your eID to access public services in other EU Member States?

Very important
Somewhat important
Not really important
Don't know

How important for you is to have a secure single digital ID that could serve for all online services (both public and private) that provides you with the control over the use of your personal data?

Very important
Somewhat important
Not really important
Don't know

How important for you is the ability to use your eID on your mobile phone?

Very important
Somewhat important
Not really important
Don't know

4. General questions about electronic trust services

The eIDAS Regulation aimed to create a European internal market for electronic trust services - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based processes.

Have you ever used electronic trust services (e.g. eSignature, eSeal or Timestamp)?

Yes

No

Don't know

To what extent do you agree or disagree with the following statements? (only one option per question)

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
The availability and offer of electronic trust services in the EU is sufficient.			**X**			
The eIDAS Regulation needs to be strengthened as a response to the COVID-19 crisis			**X**			
Providing the same legal effect to electronic trust services (e.g. qualified e-signature is equivalent to handwritten one) helped increase their take-up.			**X**			

I feel more comfortable and confident to use electronic trust services now compared to five years ago.						**X**
Public administrations should roll out more public services, making better use of electronic trust services in their contact with citizens and businesses.	**X**					

Do you think that additional trust services should be regulated at EU level?

Yes

No

Don't know

If yes, please specify the additional trust services:

INATBA members believe that there should be trust services that enable citizens and businesses to utilize self-sovereign identity technology (ie. to receive verifiable credentials from regulated trust services). These should enable: Data portability (moving data from one platform/network to another); Tracking access to personal data and giving explicit consent for using personal data; Establishing standards regarding the structure and format of data managed by Self-Sovereign Identities.

5. Specific questions on electronic identity (eID)

To answer these more specific questions would require a certain knowledge of the eIDAS Regulation.

Would you like to answer more specific questions about rules on eID under the eIDAS Regulation and the future digital identity?

Yes
No

Are you replying as:

End-user of eID (e.g. citizen, company)
Provider of online services (public sector)
Provider of online services (private sector)
Provider of Identity and Authentication solutions and / or technologies and IT solutions in this area (e.g. software, hardware, services)
Think tank, research, academic institution or individual expert
Trade/business/professional association or other interest representation organisation
Public policy maker
Non-governmental organisation
Other

If Other, please specify:

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
The number of online public services to be accessed in a cross-border context by using one of the published national eID schemes has considerably increased due to eIDAS.			X			
The eIDAS Regulation provides an adequate legal framework for cross-border electronic identification in Europe.		X				
The eIDAS legal framework for cross-border electronic identification in Europe should be strengthened as a response to the COVID-19 crisis.			X			
The scope of the eIDAS Regulation should be extended to provide a level playing field for the private economic actors operating in the field of electronic identification.		X				
The interoperability framework established by the eIDAS is optimal and supports sufficiently the mutual recognition of the eID schemes.				X		

Do you agree that the use of electronic identification to access online public services across borders contributes to:

	Strongly agree	Agree	Neither agree not disagree	Disagree	Strongly disagree	I don't know/no opinion
Enhancing user friendliness		X				
Saving time		X				
Saving money		X				
The simplification of the administrative procedure		X				
An increase of service quality		X				
An increase of service security		X				
The protection of personal data			X			
The better access to services in another EU country	X					
An increase of the certainty on the authenticity of the users' identity		X				
Enhancing clarity on the		X				

liability of the provider of the electronic identity						
The access to services to a larger group of users thanks to the uptake of eID			**X**			

In your opinion, are there currently any factors limiting the cross-border use of electronic identification?

Yes

No

Don't know

What are the factors limiting the cross-border use of electronic identification? (Multiple choice is allowed)

Lack of awareness
No need for it / Not relevant
Limited number of notified eID schemes
Lack of availability of relevant public services
Lack of trust
Preference for paper-based solutions or face-to-face interactions
Too expensive
Too complicated / not user-friendly / accessibility barriers for persons with disabilities
Privacy concerns
Legal obstacles (example: face-to-face interaction required by national legislation)
Limited scope of eID schemes notified under the eIDAS Regulation
(governmentally issued/recognised eIDs only)
Suboptimal interoperability framework 1time selected
Other

If Other, please specify:

The majority of INATBA members highlight the following factors: Lack of awareness; Limited number of notified eID schemes; Lack of availability of relevant public services. Others also identify the following as limiting factors: Preference for paper-based solutions or face-to-face interactions, Too complicated / not user-friendly / accessibility barriers for persons with disabilities, Legal obstacles (example: face-to-face interaction required by national legislation), Limited scope of eID schemes notified under the eIDAS Regulation.

To what extent do you agree that the eIDAS Regulation has achieved its objectives with regard to electronic identification?

The objectives were: to enhance trust in electronic transactions in the internal market by providing a common foundation for secure and seamless electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public online services in the EU.
The Regulation ensures that individuals and businesses can use their own national electronic identification schemes (eIDs) to authenticate when accessing public online services in other EU Member States, by establishing interoperability and enforcing mutual legal recognition of notified schemes.

Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
I don't know / no opinion

Please elaborate on how the eIDAS Regulation has/not achieved its objectives with regard to electronic identification.
Do not hesitate to further elaborate on your previous answers.

In your opinion, should the eIDAS Regulation or its implementation be improved?

Yes
No
Don't know

Which of the following corrective actions should be taken? (multiple choices can be selected)

Adopting guidelines to improve legal coherence and consistency

Further harmonisation through requirements established in secondary legislation (implementing acts), standardisation and the introduction of certification to the advantage of particularly convenient and secure solutions

A shift from voluntary to mandatory notification of national eID schemes

An obligation for Member States to make authentication available to the private sector 2times selected

Introduction of new private sector digital identity trust services for identification, authentication and provision of attributes

Introduction of an obligation for the public sector to recognise attributes, credentials and attestations issued in electronic form by trust service providers and public authorities registered as authoritative sources

Introduction of an obligation for the private sector to recognise trusted digital identities: eIDs notified under eIDAS and trust services for identification, authentication and provision of attributes

Provision of identification for non-human entities (e.g AI agents, IoT devices)

In your opinion, should there be a single and universally accepted European digital identity scheme, complementary to the national publicly issued electronic identities, allowing for a simple, trusted and secure possibility for citizens to identify themselves online?

Yes

No

Don't know

Which possible advantages of such single and uniform European digital identity scheme are important to you? (multiple choices can be selected)

Trust (Government Sponsored)
Universal Acceptance
User convenience
Better control of personal data
Increased online security
Cost savings thanks to economies of scale
Other

Please specify and/or set-out other possible advantages:

Which possible dis-advantages of such single and uniform European digital identity scheme are you concerned of? (multiple choices can be selected)

Complexity of set-up and Governance
Lack of flexibility to adapt to technological developments and changing user needs
Overlap with existing solutions
Discouragement of innovation and investments into alternative eID solutions
State surveillance concerns
Set up and operational costs
Other

Please share any additional statements, documents, position papers concerning eID under the eIDAS framework and the future of digital identity.
See Attachement 1

6. Specific questions on trust services

To answer these more specific questions would require a certain knowledge of the eIDAS Regulation.
Would you like to answer more specific questions about trust services and the eIDAS Regulation?

Yes
No

Are you replying as:

User of electronic trust services (e.g. citizen, company, public or private service provider)
Provider of electronic trust services
Supplier of technologies and IT solutions for electronic trust services (e.g. software, hardware, services)
Think tank, research, academic institution or individual expert
Trade/business/professional association or other interest representation organisation
Public policy maker
Supervisory body
Conformity assessment body
Non-governmental organisation
Other

If other, please specify:

Which of the following trust services are relevant to you? (multiple choice)

The selected trust services will trigger separate questions for each trust service regulate under eIDAS.
Electronic signature
Electronic seal
Electronic timestamp
Electronic registered delivery service
Website authentication

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	I don't know/no opinion
The eIDAS Regulation increased the availability of electronic trust services in the EU.					X
The level and scope of governance and supervision of electronic trust services established under the eIDAS Regulation are adequate to ensure harmonisation at EU level.		X			
The eIDAS Regulation has put in place conditions conducive to trust services based on decentralised solutions (including through distributed ledger technologies).			X		
The legal effect provided to trust services by the eIDAS Regulation (e.g. qualified esignature is equivalent to handwritten one) helped increase their admissibility in legal proceedings			X		
The cross-border legal effect provided to trust services by the eIDAS Regulation helped increase their take-up.			X		
The assessment procedure for becoming a qualified trust service provider is adequate.				X	
The eIDAS Regulation is a more effective tool to regulate trust services than actions taken at national level.		X			
The provisions of the eIDAS Regulation on trust services have enhanced trust in electronic transactions.			X		

Repealing the eIDAS Regulation would have negative consequences for trust services in Europe.		X			

If you have selected ELECTRONIC SIGNATURE in the previous question:
To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	I don't know/no opinion
The eIDAS Regulation has increased the availability of electronic signature in the EU.		X			
The availability of electronic signature in the EU should be extended as a result of the COVID-19 crisis.					X
The use of electronic signature has increased in Europe for the last 3 years.		X			
The eIDAS regulatory framework creates a level playing field for electronic signature in Europe.		X			
The eIDAS Regulation does not hinder technological developments in the electronic signature market.			X		

Citizens, businesses and public administrations in Europe can effectively benefit from the advantages of electronic signature.		X			
The eIDAS Regulation has ensured interoperability of electronic signature.		X			

If you have selected ELECTRONIC TIMESTAMP in the previous questions:
To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	I don't know/no opinion
The eIDAS Regulation has increased the availability of electronic timestamp in the EU.		X			
The availability of electronic timestamp in the EU should be extended as a result of the COVID-19 crisis			X		

The use of electronic timestamp has increased in Europe for the last 3 years.		X			
The eIDAS regulatory framework creates a level playing field for electronic timestamp in Europe.		X			
The eIDAS Regulation does not hinder technological developments in the electronic timestamp market.			X		
Citizens, businesses and public administrations in Europe can effectively benefit from the advantages of electronic timestamp.			X		
The eIDAS Regulation has ensured interoperability of electronic timestamp		X			

Please specify which additional trust services should be regulated at EU level:(multiple choices needed)

Electronic identification and authentication

Provision of trusted attributes (uniquely linked to a verified identity – e.g. proof-of-age, credentials – professional qualifications, entitlements – Know-

Your-Customer) 2 times selected

eArchiving 1 time selected

Delegated management of signature keys

Operation of distributed ledgers storing electronic evidences 3 times selected

Operation of identity hubs storing personal data of behalf of the users 2 times selected

Other

No need for additional trust services, the current scope is sufficient

If other, please specify:

The majority of INATBA members believe that the operation of distributed ledgers storing electronic evidences should be regulated. Others believe the following trust services should also be regulated: Electronic identification and authentication, provision of trusted attributes (uniquely linked to a verified identity – e.g. proof-of-age, credentials – professional qualifications, entitlements – KYC), operation of identity hubs storing personal data on behalf of the users.

Do you agree that the use of trust services established by the eIDAS Regulation contributes to:

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree	I don't know/no opinion
Enhancing user friendliness						X
Saving time		X				
Saving money		X				
The simplification of the administrative procedure						X
An increase of service quality		X				
An increase of service security		X				
The protection of personal data			X			
Ensuring legal certainty		X				

Do you think the legal effect provided to electronic documents by the eIDAS Regulation has effectively increased their take-up and admissibility in legal proceedings?

Art. 46 of the eIDAS regulation states that "An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form."

Strongly agree

Agree

Neither agree nor disagree

Disagree

Strongly disagree

I don't know / no opinion

In your opinion, are there any factors limiting the use of electronic trust services?

Yes

No

Don't know

What are the factors limiting the use of electronic trust services? (multiple choice)

Lack of awareness 2 times selected
No need for it / Not relevant
Lack of availability for relevant services 2 times selected
Lack of trust or fraud concerns 1time selected
Preference for paper-based solutions or face-to-face interactions 2 times selected
Too expensive 1 time selected
Too complicated / not user-friendly / accessibility barriers for persons with disabilities
Privacy concerns
Not enough legal certainty
Other

If Other, please specify:

The majority of INATBA members highlight the following as the factors that limit the use of electronic trust services the most: Lack of awareness, Lack of availability for relevant services, Preference for paper-based solutions or face-to-face interactions. Others also indicate: Lack of trust or fraud concerns, and the high costs.

To what extent do you agree that the eIDAS Regulation has achieved its objectives with regard to electronic trust services?

The objectives were: to seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure and seamless electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the EU.
The Regulation ensures the development of a European internal market for electronic Trust Services (electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication) recognised across borders with the same legal status as traditional paper based processes.

Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
I don't know / no opinion

Please elaborate how the eIDAS Regulation has/not achieved its objectives with regard to electronic trust services.
INATBA members believe it has not provided for mass adoption.

How could the eIDAS Regulation or its implementation be improved with regard to trust services?
INATBA members believe it could be improved with DLT signatures.

Please share any additional statement, document, position paper regarding trust services and eIDAS.

The maximum file size is 1 MB
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed
See Attachment 2

Brussels, 2 October 2020

INATBA Identity WG Response

to the EU Commission Open Public Consultation

on the eIDAS Regulatory Framework

Attachment 1

The INATBA Identity Working Group has a high interest in getting decentralized open standards based identity to be accepted under eIDAS and included in the trust services and eID concepts.

The Working Group supports EBSI-ESSIF in this direction, but also underlines the need for more transparency and SME participation in EBSI-ESSIF.

The current eIDAS approach to electronic identification is based in a federated identity management system, setting up an identity metasystem that allows the cross-border authentication using notified electronic identification means. This identity metasystem is technically based in two models - the proxy node approach and the middleware approach - that present relevant challenges for effective adoption by private sector bodies or social perception of privacy risks, among others.

1. **Adapt the eIDAS electronic identification concept to SSI**

SSI is a technological approach that may help overcome these challenges, complementing the current interoperability specification developing the eIDAS Regulation, as stated in the SSI eIDAS Legal Report (https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report).

While it may be argued that it is not strictly necessary to modify the current eIDAS Regulation to adopt the SSI approach for electronic identification, it would be convenient to adapt the language of the Regulation, which resembles the delegated authentication approach, to facilitate the adoption of SSI solutions. One example, albeit not the only one, relates to the obligation of Member States, and their corresponding liability, to offer an online authentication facility. Sections 8.1 and 9.1 of the SSI eIDAS Legal Report provide insight in this respect.

2. **Extend the eIDAS notification procedure to all types of identity credentials**

But the real innovation provided by SSI technology allows a transformative view with respect to the eIDAS Regulation, which could be extended to support legally valid, crossborder, identity attestations (e.g. diplomas, age verification, etc.).

As explained in section 10.1 of the SSI eIDAS Legal Report, eIDAS does not cover identity management in a wide sense, but just electronic identification. Thus, it is not immediately applicable to the issuance and sharing of other verifiable credentials/presentations (EBSI ESSIF Verifiable Attestations). This is reasonable from the perspective of the legal regime of the content of these credentials (e.g. a diploma), but it makes difficult using them in a cross-border scenario, because of the existence of multiple, sectoral, regulations.

One possibility to solve this problem is to extend the legal approach and governance rules already existing in the eIDAS Regulation, to regulate a general framework for the lifecycle of verifiable credentials/presentations used for purposes different to electronic authentication.

The current legal approach in the eIDAS Regulation is very concrete and detailed: it contains legal definitions related to electronic identification (electronic identification scheme, electronic identification means, personal identification data) and authentication; defines processes, levels of assurance, interoperability and governance rules. In short, a full legal trust framework for cross-border authentication, an important part of identity management.

The proposal, in this scenario, would be to create a parallel trust framework for issuing and sharing other identity attributes. This objective cannot be accomplished in the same way as the current approach for electronic identification, because the semantics and rules of these other identity attributes are quite different. Although they identify a person, in a very wide sense, they are not used for identification and authentication, but the legal technique to support the legal validity of these credentials would be the same; that is, the notification procedure would be used for all types of identity credentials, as a was to ensure their quality, security and interoperability.

The analysis of any sectoral framework regulating identity credentials (e.g. diplomas in support of professional qualifications accreditation, a use case included in EBSI) shows the complexity of transforming the classical certifying documents normally issued by Public Administration. To facilitate a quick transformation into Verifiable Attestations, a new equivalence rule could be proposed, in the sense of authorising the use of a Verifiable Attestation according to the (new) eIDAS Regulation whenever a legal norm requires a document certifying an identity attribute for a natural or a legal person.

The following recommendations could be pertinent:

- Propose modifying Chapter II of the eIDAS Regulation with the necessary Articles to extend the existing trust framework embodied in the eIDAS Regulation for electronic identification, to include a common framework for identity data sharing under the control of natural or legal persons, sustained by a ledger conceived as a public good.
- Create a legal rule, based in the equivalence principle, to authorise the use of a Verifiable Attestation according to the (new) eIDAS Regulation whenever a legal norm requires the presentation of a document certifying a natural or a legal person identity attribute.
- Member States should be mandated to admit notified Verifiable Attestations, substituting the paper or electronic documents (such as diplomas) containing the identity attributes.
- Create a specific legal rule authorising the use of an advanced or qualified electronic seal for the issuance of Verifiable Attestations, whenever the Law applicable to the form of the document mandates the use of a signature.
- Define a governance framework for a trusted issuers ledger providing verifiable attestations, considering the possibility of managing the lifecycle of these issuers by Member States with the intervention of the European Commission.

Brussels, 2 October 2020

INATBA Identity WG Response

to the EU Commission Open Public Consultation

on the eIDAS Regulatory Framework

Attachment 2

Despite the fact that the eIDAS Regulation does not formally define what trust services are, they can be conceptualised as those technologies that can be trusted, therefore modifying the user's perception regarding the vulnerability of a process to which they are incorporated.

To this end, users must be able to recognise a trust service, in fact, as secure and reliable enough. To do this, the approach of the eIDAS Regulation is the creation of a reinforced level of trust services (qualified trust services), which is significant in the sense that the trust in these services seems to be born from the fact that they are legally regulated, rather than only in their own technical characteristics.

It should also be noted that the eIDAS Regulation contains a closed list of trusted services in order to delimit the scope of the uniform European regulation but that Member States may define other trust services as well as maintain (or introduce) national provisions, in accordance with Union law, concerning trust services of confidence, provided that such services are not fully harmonised by this Regulation, considerations which show the central objective of the regulation, which is none other than to guarantee the free movement of these services in the internal market, by means of a minimum set of harmonised standards.

One consequence of this model is the more than possible divergence in the catalogue of trust services in the different jurisdictions of the European Union, as the business sector is constantly generating new services, based on technological innovation. For instance, Belgium has regulated a national trust service, consisting in a secure document archive, with a specific legal effect, both as non-qualified and qualified service.

1. Adapt the eIDAS qualified certificate concept to SSI

Apparently, in this construction, it does not fit that the regulation of the identification proof has not been classified as a typical trust service, since it is not expressly included in the definition of these services, but in reality this is not entirely true. There are harmonised trust services in the eIDAS Regulation that have, among their typical legal effects, that of allowing electronic identification. This is the case of the issuance of certificates of electronic signature of a natural person, a trust service harmonised by the eIDAS Regulation, which confirms the identity of said natural person; and in the same way it happens with the certificate of electronic seal of legal person, which confirms its identity. Therefore, these trust services, which can be subject to qualification, allow electronic identification, at least in connection with said electronic signature or electronic seal.

Similarly occurs with the authentication –which actually fulfils the identification function– of websites, which is dealt with in the eIDAS Regulation, unlike the electronic identification of natural or legal persons, as a harmonised trust service, including its qualification.

Section 9.2 of the SSI eIDAS Legal Report considers the possibility of considering specific DID methods plus specific types of verifiable credential as a “qualified certificate”, both for natural and for legal persons, based on a technologically neutral, wide, interpretation of the eIDAS Regulation (more specifically, of the “certificate” definition).

As qualified certificates confirm the identity of the subject (signatory or seal creator or website name owner), this specific combination of a DID method and a verifiable credential (or, depending on the underlying technology, a verifiable presentation embodying a set of verifiable credentials) would benefit from the legal effect defined for qualified certificates, and would also support advanced and qualified signatures and advanced qualified electronic seals in blockchain transactions.

This type of credential or presentation could also be notified as an electronic ID means, when including the minimum data set.

Moreover, this approach would facilitate transitioning from PKI to DPKI and SSI systems, while maintaining and even fostering a valuable market and reusing a convenient and proven supervisory and liability regime.

The following recommendations are pertinent:

- Modify the certificate definition, in the sense of understanding the expression “an attestation” may be referred to the combination of a verifiable credential and one or more DID documents (“SSI eIDAS qualified certificate”).
- Provide guidance for the definition of DID methods for the issuance and lifecycle of SSI eIDAS qualified certificates including those to be also admitted as verifiable IDs.
- Develop a governance framework for a trusted issuers ledger for qualified trust service providers, considering the possibility of managing the lifecycle of qualified trust services by supervisory bodies of Member States.
- Modify Article 22 of the eIDAS Regulation and withdraw Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists.

2. Regulate the issuance of Verifiable Attestations as a trust service

As indicated in section 10.2 of the SSI eIDAS Legal Report, following the legal logic of qualified certificates deployed as a DID method plus a verifiable credential under specific rules, it could be possible to define a new trust service, oriented to the issuance of verifiable credentials containing identity attributes (other than foundational identity attributes contained in VCs issued as qualified certificates).

Main benefits include leveraging all the common rules, the supervisory framework and the liability model set up in Chapter III of the eIDAS Regulation (a legal trust anchor) for issuing identity attributes in a separated instrument (the Verifiable Credential).

If it is legally acceptable to issue a qualified X.509 certificate with additional attributes, under the liability regime of the current eIDAS Regulation, it should also be possible to issue these additional attributes in a separate artefact (the Verifiable Attestation). This could be implemented considering the qualified certificate (SSI eIDAS qualified certificate) is formed by a Verifiable ID and one or more Verifiable Attestations issued by the same entity, but Verifiable Attestations may also be issued to a subject that already has an SSI eIDAS qualified certificate.

One of the foundational bases of SSI consider that identity is a social construct, formed by multiple relationships conforming a graph, that conform a wide conception of digital identity. In that view, it does fully make sense to promote that any entity issues verifiable credentials, especially if they are ensured by a legal regime.

A lot of cases exist where it is convenient to issue Verifiable Attestations as an independent trust service, such as customer due diligence evidential identity information, allowing the possibility of reusing the very costly Know Your Customer processes.

The adoption of this measure would increase the market size for EU qualified trust service providers, helping them compete in a global scale with other SSI network's trust models, requiring issuers to be authorised by the network's stewardships, preventing the risk to shifting dependency from trust anchor stores to decentralised networks trusted issuers registries.

On the other hand, this possibility could also facilitate natural and legal persons to share their Verifiable Attestation issued by qualified trust service providers (probably in collaboration with third parties) with public sector bodies. An example would be to share a bank account information contained in a Verifiable Attestation with a public sector body, in a voluntary basis.

In case this qualified Verifiable Attestation has also been notified, then this credential would benefit from the legal benefit of that process.

The following recommendations apply:

- Propose modifying Chapter III of the eIDAS Regulation with the necessary Articles to define and regulate a new trust service, qualified and non-qualified, with respect to Verifiable Attestations.
- Propose defining the legal effect of qualified Verifiable Attestations of presuming the authenticity of the identity attributes contained therein.
- Create a specific admissibility and non-discrimination rule with respect to non-qualified Verifiable Attestations.

3. Regulate a specific type of DLT node as a trust service

Finally, we may envision the possibility of extending the eIDAS Regulation to a specific trust service consisting on the operation of a specific type of node, for a specifically designed DLT, tailored for the generation of electronic evidences, as analysed in section 10.5 of the SSI eIDAS Legal report.

DLT providers own and operate one or more nodes within DLT systems and DLT networks. They agree to create/instantiate nodes, join networks, pay for, and handle legal agreements for joining the network. Even if these systems are said to be “trustless”, in the sense of not needed a third party, they are still provided by someone, in many cases as an economic activity. The fact that they need to necessarily cooperate in the execution of the consensus algorithm (to name an example), does not mean they should not have legal obligations nor bear liability in case of damaging third parties, at least with respect to their functions, and regardless of other DLT systems roles, e.g. a DLT governor.

Currently, this service must be considered as an information society service, subject to the general provisions contained in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), as implemented in national legislation, and thus, any service provider in a DLT system will need to comply with the corresponding legal requirements , as applicable. And in case, any entity acting in a DLT system that produce any damaged to a third party is subject to non-contractual liabilities.

The logic of any trust service in the eIDAS regulation, especially those that are subject to qualification, is to determine a set of rules to ensure its trustworthiness, in view of defining a specific legal effect for it, or to ensure legal certainty and consumer protection.

This legal logic is perfectly applicable to the provision of services in a DLT, with some adjustments. For instance, qualification should be granted for each DLT node forming the network, with a minimum number of them, according to the DLT governance framework set up (for instance, before launching the genesis block).

The advantage of this approach is that it would allow setting up a series of legal requirements aimed to deploy distributed networks that balance the public/legitimate interest in the legal certainty of electronic evidences, with the rights and expectations of all parties.

Thus, as DLT networks provide many of the core services for applications, this legal framework could foster the availability of baseline services on top of which other services would be reliably deployed (namely, identity and signature/seal services, timestamping services or electronic registered delivery services).

Regulation would cover aspects such as governance and consensus models, time synchronization, crypto security, software certification, then need to get an administrative authorisation to make a fork, etc., but also legal limits to anonymity and some privacy rights, such as right to modification or right to erasure, attending to the final purpose of these specific DLT networks, which is to provide trust to transactions.

The following recommendations may be considered:

- Propose modifying Chapter III of the eIDAS Regulation with the necessary Articles to define and regulate a new trust service, qualified and non-qualified, with respect to DLT systems addressed to consumers.
- Consider imposing balanced limitations of privacy rights when using qualified DLT systems trust service, attending to the public interest in electronic evidence registered to provide legal certainty.

Contact details:

Website	inatba.org
Identity WG Co-chairs	identity-wg-cochair@inatba.org
Press	pr@inatba.org
Join INATBA	membership@inatba.org