KNB
Koninklijke Notariële Beroepsorganisatie

The Hague, August 30th 2021

Remarks of the Royal Dutch Association of Civil-law Notaries (KNB) on COM(2021) 281, the "*amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*"

The KNB reviewed the draft amendment of the "*amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity"* regulation published on the 3rd of June 2021. We would like to emphasize that we support the proposal of the Council of the Notariats of the European Union (CNUE) for an extension of the eIDAS level 'high'. This extension should consist of *en vivo* face-to-face identification, biometric aspects and additional safeguards to prevent fraud and to protect the EU citizen as much as possible.

Besides the CNUE contribution the KNB has the following seven remarks regarding the amendment of the eIDAS regulation:

1. Adding additional services which could negatively influence eIDAS adoption

The KNB is worried that only 59% of the EU residents have the ability to apply for an eID in their own country. This results in an even lower adoption rate of eID's by EU citizens. To our surprise no technical standard clarifications were issued to assist the development and thus the availability of new eID's. Instead additional mandatory products were added to the draft regulation. Even though we as KNB fully support identity wallets and welcome their proposed legal status. We would like to emphasise that the development of those newly added products will add a considerable strain on development resources. We strongly recommend addressing the increase of the availability of eID's first. Especially in the area of interoperability between member states clear standards and guidelines are missing.

After the amendment of the regulation will become applicable, the member states will have only twelve months to comply with the new regulation. Moreover, the Commission has to establish technical and operational specifications and references to standards within six months after the Regulation enters into force. Thus, creating a time frame of only six months for organisations to interpret, design, develop and test their digital identity wallets. This time pressure can have two unfavourable consequences. Firstly, the possibility arises that member states are not able to perform the audit process at the desired security level due to the obligation to provide an eID and digital identity wallets (art 6a-6d) within the given timeframe. Secondly due to the time constraint it might be in the advantage of big tech companies with substantial resources to create a digital wallet within this short timeframe.

To increase this development timeframe, we propose to start a consolidation on the technical and operational specifications as soon as possible (Q1 2022) and release a preliminary report shortly after. Besides, we propose the following two changes: to change the timeframe from 12 months to **24 months** for the mandatory availability of Digital Identity Wallets and that the 12/24-month time frame to have an identity wallet available starts when the technical and operational specifications are published.

The proposal states that the European Digital Identity Wallet may be issued by: (a) a Member State; (b) under a mandate from a Member State; (c) independently but recognised by a Member State. This means that a Member State is not obliged to open its Electronic Identification scheme to other

(private) parties. To increase the availability of the European Digital Identity Wallet and other eID means, we would like to propose that Member States should at least be obliged to involve (private and public) market players which are ready to join a national electronic identification scheme.

By this it is prevented that suddenly existing technologies become obsolete due to a governmental act and the development of new technologies will be enhanced due to increased legislative certainty.

2. Embedding notarial power of representation in the proposal

An earlier report by the European Commission, entitled "SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market," (April, 2020) suggested a possible (crucial) role for the notary public in an attribute attestation:

"A qualified electronic signature shall have the equivalent legal effect of a handwritten signature (Article 25 (2) of the eIDAS Regulation). Thus, using an electronic signature will only make sense when the verifiable credentials incorporates a legal act by a natural person issuing the credential. For example, a Public Notary could issue a verifiable credential containing a notarial power of representation."

KNB believes that civil law notaries can play an important role in legal transactions by providing legal certainty through legal obligations to authenticate and verify the identity of persons. The law grants the notary several exclusive powers in the field of legal acts that may only take place in a notarial deed. Has the European Commission taken the conclusion of this report into consideration? KNB proposes to embed the role for notaries in the new eIDAS regulation as suggested in the above-mentioned report.

3. Authentic source

The proposal (Article 45 d) also refers to an authentic source that contains attributes about persons. Recital 46 contains the following definition of authentic source:

(46) 'authentic source' is a repository or system, held under the responsibility of a public sector body or private entity, that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in national law;

KNB would like to emphasize that the core function of the notary is the provision of legal certainty and that it fulfils this function by recording various legal acts in notarial deeds, including the verification and recording of attributes of persons. KNB sees a role for the notary in the creation and maintenance of this authentic source. KNB would request that the proposal suggests the role of the notary public as holder and keeper of the authentic source.

4. Mandatory acceptance for a request for face-to-face legal acts

KNB points out that the notary always has and should retain the authority to request the person involved to appear in person to verify the identity of the person and the will and competence for the desired legal act(s). KNB asks you to include in the proposal that in the case of notarial services physical presence may be deemed necessary because it is in the best interest of the person(s) concerned. In such case that person may be requested to appear physically. Therefore, propose to add a new paragraph 4 to Article 8:

"For passing of notarial deeds the notary may always request the persons involved to appear physically in order to verify the will and competence of these persons. "

5. Technical specification shortcomings undermine notary proceedings

KNB values the abilities of digital identities and signatures but acknowledges several of its limitations. With notary proceedings requiring unconditional identification certainty in the physical world, the digital identification means should increase or at least match that level of certainty. However, the eIDAS level 'high' technical specifications potentially do not provide the same level of certainty as identification by notaries in the physical world. We have found several potential imperfections in the eIDAS high technical specification (Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015) regarding authentication mechanisms.

2.3.1 Authentication mechanism assurance level High (Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015):

"Level substantial, plus:

The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms."

The technical specification does not cover the possibility that another person than the owner of the eID has access to the eID. For instance, a person can use a stolen eID to create a shell corporation in the name of the unaware owner of the eID. The illegitimate person logs in using the stolen eID to set up a legal entity for a company, in accordance with amending Directive (EU) 2017/1132. Further it is quite common that persons voluntarily give someone else control over their credentials. The KNB recommends an extension of the technical specification, to protect a person against the use of their eID without their knowledge in high impact transactions. The KNB proposes the following two additions to the technical specification for the assurance levels of electronic identification:

2.3.1 Authentication mechanism Assurance level High to achieve this protection:

"2. The authentication mechanism implements security controls for the verification of the electronic identifications means, so that it is highly likely that the person from whom the eID is used is present at the moment that the eID is verified.

3. In the case of a video conversation the relying party must be able to perform an additional verification using biometrics stored in an official identification document to verify that the person participating in the video call is the owner of the eID."

6. Sector specific requirements in related legislation

We have found that Article 2 paragraph 3 does not provide the expected security regarding the notary procedures as it deems to do.

"This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to sector specific requirements as regards form with underlying legal effects."

The KNB would like to remark that the *"amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law"* made it clear that the eIDAS levels can operate stand alone and affect national law through directives. Thus, effectively contradicting with Article 2 paragraph 3 and compromising the security given under for example the Dutch national notarial laws. Therefore, the

KNB would like to emphasize that directives referring to the eIDAS regulation should not deviate from the principals of Article 2 paragraph 3.

7. Unclear reference to technical standards

eIDAS is currently comprised of the main body of the law text and is complemented by a number of Implementation Decisions. Each of these Implementation Decisions refer to a number of technical standards and the latter again to other technical standards. This generates a complex and large number of choices to be made in the technical realisation of eIDAS trust services. It is not clear if these choices are considered to be inclusive or optional. If these are inclusive, this would lead to high costs and complex systems to achieve full interoperability. If these are optional any member state or trust service provider can select a selective different subset leading to a strongly diminished level of interoperability. Although the European Network and Information Security Agency (ENISA) is publishing guidance on this subject it is hardly complete and member states can still follow their own path.

The eIDAS set of standards seems to be still in development, which is a good thing. However, this means that it is very difficult to maintain a consistent and up to date view on “valid” standards. It would be beneficial for implementers, trust service providers, auditors etc. to have a single register of all eIDAS related standards and their status maintained by for example ENISA. This register should have a legal status comparable to the eIDAS regulation and comply with the Implementation Decisions.