



AIMA

167 Fleet Street, London EC4A 2EA, UK

+44 (0)20 7822 8380

info@aima.org

aima.org

Jan Ceyskens
Head of Unit, Digital Finance
DG FISMA
European Commission
Rue de Spa 2
1000 Brussels
Belgium

Submitted via feedback portal and by email to jan.ceyskens@ec.europa.eu

26 August 2021

Dear Mr Ceyskens,

AIMA feedback on the proposal to revise the framework for a European Digital Identity (COM(2021) 281 final)

The Alternative Investment Management Association (AIMA)¹ welcomes the opportunity to provide feedback to the European Commission's "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity" (the "Proposal").

We fully support the European Commission in its objective to create an EU-wide digital identity framework as part of the EU's Shaping Europe's Digital Future strategy. Indeed, in a white paper that we published in 2020, and which we have previously shared with you and your colleagues within the European Commission, we outlined several options to improve the customer due diligence (CDD) process through the use of a multi-jurisdictional, digital identification solution.

To that end, we believe that the European Digital Identity framework should be principles-based, and as open and inclusive as possible in order to facilitate a more global, uniform approach to digital identification and verification and an improved AML/CFT ecosystem. This would ensure that

¹ AIMA, the Alternative Investment Management Association, is the global representative of the alternative investment industry, with more than 1,900 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than \$2 trillion in assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA works to raise media and public awareness of the value of the industry. AIMA set up the Alternative Credit Council (ACC) to help firms focused in the private credit and direct lending space. The ACC currently represents over 170 members that manage \$400 billion of private credit assets globally. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For further information, please visit AIMA's website, www.aima.org.

both EU and non-EU legal entities and natural persons have equal access to the benefits that the Proposal aims to introduce. A more principles-based approach to the use of digital identities would allow all users, and service providers, regardless of where they are located, to access and contribute to a convenient, trusted, secure and innovative authentication and identification framework. Moreover, such an approach would also facilitate the inter-operability of the digital identity schemes and the use of electronic identity services from non-EU service providers by EU entities and natural persons, and, correspondingly, the use of non-EU identity services to supplement those that are available in the EU.

In order to achieve this, we have a few questions and concerns which we would ask the European Commission to share with the European Parliament and European Council as they prepare for their legislative debate.

Equal access for nationals and residents

In various places throughout the Proposal, there are references made to equal treatment of “nationals and residents” and “citizens and residents”. Presumably, the category of “residents” will include citizens from other EU Member States, dual citizens (e.g., natural persons born outside the EU but who also hold citizenship in an EU Member State) and persons in a Member State legally pursuant to any one or a variety of long- and short-stay visa programmes. However, the Proposal only seems to make provisions for trust services and providers of electronic attestations of attributes established in the EU. If non-EU entities can meet the required technical standards and data privacy/protection requirements, we believe there is no good reason to exclude them from the ecosystem. If non-EU entities are not permitted, it is likely that equal treatment of some residents will not be possible to achieve. Moreover, if use of the digital identity wallets is mandated (e.g., through the Anti-Money Laundering Regulation (see below)) and non-EU attestations, attributes and credentials are not included, then some residents may be by default excluded from certain types of vital services. In addition, non-EU citizens, non-EU residents, EU legal entities with non-EU directors or beneficial owners and non-EU legal entities may be entirely foreclosed from accessing the services of EU financial institutions and other obliged entities under the Anti-Money Laundering Regulation which is surely an unintended result, and which suggests a more open framework approach to electronic identification may be justified and appropriate. In the context of the alternative investment industry, the exclusion of non-EU entities and non-EU attestations would be highly disproportionate as EU-based trust services and providers of EU electronic attestations would then no longer be in a position to service their non-EU investors or contract non-EU service providers.

Identification of providers and the requirements applicable to each

In the global alternative investment industry, investment funds and fund managers contract third-party service providers, such as fund administrators, to perform a range of tasks, including conducting CDD activities and other anti-money laundering, know your customer and counter terrorist financing related services. While the Proposal names many types of potential providers, it does not provide clarity about their respective roles and how they are meant to interact as part of an integrated ecosystem.

For example, Recital (27) states that “[a]ny entity that collects, creates and issues attested attributes such as diplomas, licences, certificates of birth should be able to become **a provider of electronic attestation of attributes**” (emphasis added). This statement appears to envision a

university or professional body issuing diplomas, certifications, licences or other types of credentials (or attributes – see above) would have a particular role in the system laid out in the Proposal – i.e., provider of electronic attestation of attributes. However, the Proposal does not specify what the details of that role are, how such entities are meant to interact with the broader ecosystem of service providers and trust services and, importantly, what technical standards are required. These same providers are also likely to be the relevant “authentic sources” for these types of credentials/attributes, but again there is no further detail on the manner in which electronic authentication is to be provided. Recital (4) states that “[p]roviders of electronic attestations of attributes should benefit from a clear and uniform set of rules and public administrations should be able to rely on electronic documents in a given format”. We agree, but, again, the Proposal does not appear to cover this.

Other examples include the “providers of electronic identification means and electronic attestation of attributes” in Recital (6), the general “service providers” in Recitals (8) and (17) and “identity or attestation of attributes’ [sic] service providers” from Recital (30).

Communication of a service provider’s intent to rely on the European Digital Identity Wallet

Under the Anti-Money Laundering Regulation proposal (COM/2021/420 final), Article 18(1)(d) suggests that there are going to be some electronic identification means and relevant trust services that “must feature” in order to satisfy the CDD requirements of the Anti-Money Laundering Regulation.

If every obliged entity under the Anti-Money Laundering Regulation is required by that Regulation to use certain electronic identification means and relevant trust services, we believe this use case and any other mandatory use cases should specifically be carved out of the requirement in Article 6b of the Proposal which would require relying parties to notify a Member State that it intends to rely on the European Digital Identity Wallet.

We also believe a specific carve out from Article 38, 39 and 40 of the Anti-Money Laundering Regulation proposal (i.e., the provisions on reliance and outsourcing) is needed to accommodate reliance on the European Digital Identity Wallet when used in accordance with the Proposal. Without this, the level of trust in the wallets envisioned by Recitals (9)-(11) is unlikely to develop.

Attributes vs. credentials

In Recital (4) a university degree is identified as an attribute. Further, Recital (27) states that “[a]ny entity that collects, creates and issues attested **attributes such as diplomas**, licences, certificates of birth should be able to become a provider of electronic attestation of attributes” (emphasis added). However, an “attribute” is defined as “a feature, characteristic or quality of a natural or legal person or of an entity, in electronic form” whereas a “credential” is “a proof of a person’s abilities, experience, right or permission”. On these definitions, a university degree or diploma seems more of a credential than an attribute. We note that the Proposal as a whole is silent about the attestation of credentials, but perhaps this is an unintended outcome given the text of Recital (7) which names a number of items which are credentials and not attributes on the definitions provided. In our view, electronic attestation of credentials should be included in the Proposal.

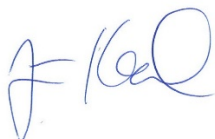
Legal persons

It is not clear from the Proposal who the “user” is when considering legal persons for purposes of digital identification. Certainly, there will be natural persons associated with these records – often more than one in fact. How would privacy permissioning work? Do individual natural persons have to give permission for other associated natural persons to see information about them in connection with the identity of the legal person? What if an associated natural person objects to this or does not provide the necessary authorisation for the release of the relevant information from that natural person’s digital identification wallet? What if one or more of the associated natural persons is not an EU citizen or resident?

It is also not clear whether it is intended that the wallet would be tied to a mobile phone app/SIM card. If this is the case, how would this work in the context of a legal person? If the information is not meant to be tied to a person’s SIM card and is instead to be stored on the cloud, a website portal alternative would make sense, especially in the context of use by legal persons.

We would be happy to elaborate further on any of the points raised in this letter. For further information, please contact Jennifer Wood, Managing Director, Global Head of Asset Management Regulation & Sound Practices, at +44 (0) 20 7822 8380 or jwood@aima.org.

Yours faithfully,

A handwritten signature in blue ink, appearing to read "J. Król".

Jiří Król
Deputy CEO, Global Head of Government Affairs
AIMA