Response of the Global Legal Entity Identifier Foundation (GLEIF) to the European Commission for the Inception Impact Assessment – Revision of the eIDAS Regulation – European Digital Identity (EUid)

September 2020

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the Inception Impact Assessment – Revision of the eIDAS Regulation – European Digital Identity (EUid). GLEIF will focus its comments on the use of the LEI in eIDAS.

Currently, the LEI is already accepted as an optional attribute for legal entities' data sets in transactions between eIDAS nodes, i.e. interfaces between national eID infrastructures. The LEI can be used within eIDAS-compliant digital certificates as the eIDAS Regulation includes a tag for digital identification tools such as the LEI to be embedded within certificates and company electronic seals to support identity validation and management. For example, GLEIF 2019 Annual Report showcased by ESMA for its compliance with the European Single Electronic Format (ESEF) is digitally signed by GLEIF's executive officers with eIDAS compliant digital certificates including the LEI.

Given the Commission considers a more ambitious legislative intervention to the eIDAS Regulation, GLEIF suggests that a more prescriptive direction from the Commission is necessary for untapping the benefits for the end-user and the whole ecosystem. Making the use of the LEI as mandatory in legal entities' data sets in transactions between eIDAS nodes would further increase the interoperability of the eIDAS framework, making cross-border electronic transactions more efficient and secure. As noted in the consultation document, in a hyper-connected economy, digital identity (digID) is becoming a critical enabler of digital transactions. But this is only true if the digital identity is set up structurally to maximize interoperability across EU member state borders and ideally with non-EU countries. The current mutual recognition of eIDs does not help different identifiers to recognize each other in digital platforms. Given the regulation intends to extend its application to the private sector practices such as online banking or online shopping, a global standard, as opposed to regional or local ones, for entity identification can maximize the cross-border interoperability.

Regarding cybersecurity, the use of the LEI allows for a persistent and reliable identification code to be present throughout successively issued digital certificates, thus enhancing trust in internet transactions and providing reliable and trustworthy information on the ownership and authenticity of electronic documents and, thereby transactions. Furthermore, the Global LEI System is overseen by regulators from around the world (see LEI ROC members for further detail), including the European Commission, resulting in a highly regulated ecosystem of legal entity identification management. Lastly, including the LEI within digital certificates establishes a verified link with the physical identity of a company thereby reducing cybersecurity threats.

Furthermore ,incorporating the LEI within digital certificates enables users to achieve the tasks of identity verification, authentication, and authorization as well as content processing in a digital environment. By digitally signing the GLEIF Annual Report 2019, GLEIF demonstrates how to incorporate this additional best practice step, beyond compliance with ESEF, to enable end user trust in the

authenticity and integrity of the Annual Report and end-to-end machine processing of the document. Specifically, any recipient of the GLEIF Annual Report can first parse the certificate and tie that certificate to the filing, in order to confirm the company filing is indeed authorized by a legal representative of the company. Additionally, the recipient then can process the entire financial report in a fully automated fashion to understand the financial position of the legal entity. Lastly, the recipient of the report could aggregate internal information on financial transactions with the legal entity that are tagged with the LEI and establish, again in a fully automated fashion, the entire risk profile of the recipient with the legal entity.

GLEIF strongly recommends the European Commission to follow option 2 for the roadmap and to consider harmonization of legal entity datasets as a priority. This would enable a **stronger mandatory usage of the LEI code** in the digital certificates that need a trusted company identification such as qualified (or advanced) business stamps, qualified (or advanced) legal representative certificates, and SSL EV that identify companies. A prescriptive approach by the Commission would remove ambiguity and bring further standardization in the application of eIDAS trust services in private sector solutions such as KYC processes in banking and finance where trusted entity identification is needed.

The eIDAS framework, while established for the EU member states, has the potential to be adopted by other nations as well. Using the LEI brings global interoperability for counterparties outside Europe naturally. Therefore the advantages of having one global neutral organization ID, the LEI code, benefits EU companies when identifying foreign companies and also works among other countries in the world. This accelerates and bring robustness in the rapid digital trusted identification of companies.

GLEIF would like to provide an example where the option 2 approach could help to improve interoperability across the EU Single Market:

> The Revised Payment Services Directive PSD2 introduces a mix of approaches for identifying legal persons. For example, it introduces a new identifier for Third Party Payment Service Providers (TPPs) (the PSP identifier) – this is administered and maintained nationally by the National Competent Authority (NCA). The PSP identifier must be embedded in the TPP's eIDAS/PSD2 Certificate to enable authentication between TPPs and banks. So within one regulation the following results:
>
> - the eIDAS/PSD2 certificate is not usable for any other digital transaction within the EU or beyond EU borders partly because it contains an identifier customized for the PSD2 implementation;
> - each NCA maintains a register with its own identifiers for banks, TPPs, and the NCA itself thereby rendering it difficult to aggregate data within the PSD2 ecosystem;
> - the PSP ID identifier cannot be used to connect to other data sources, enable analysis, or facilitate any other digital communications outside the PSD2 protocol.
>
> What if the LEI were used instead? The eIDAS/PSD2 certificate could be parsed and, using the publicly available LEI lookup API, banks could get a clearer picture of the TPP with which they are engaging TPPs would not need to put in place another process for managing another organization identifier. NCAs also could implement a less complex structure for recognizing TPPs. In total, all parties gain in efficiency and the PSD2 framework is rendered more interoperable, thereby also facilitating a more integrated EU payments market.

How could this be enabled via **option 2**? Per the scope of option 2, the eIDAS framework could be extended to make the LEI mandatory.

Moreover, from an end user perspective, 'once-only-principle' should be essential. Given, there is a strong support in the EU for making the LEI a necessary component for the creation of digital financial identities, a clear mandate for the LEI can significantly reduce the complexity and cost – both people and technology-related – associated with due diligence and validation of customers, partners and suppliers. As the EU seeks to deepen its single market, its businesses – of all sizes, but particularly SMEs - would benefit from having a single supra-EU entity identifier – connecting up the various national identifiers that exist today.

Therefore, option 2, in which the LEI code becomes mandatory effectively would create the cross-border interoperability both within and outside the EU.

Regarding option 3, DG CNECT may consider extending the vision to include persons acting on behalf of organizations. The recently updated ISO 17442 standard for the LEI includes rules how the LEI and the role of the person should be represented in public key certificates. This would enable company officers to digitally take action on behalf of a firm, for example, signing contracts, submitting regulatory filings or approving payments. As the consultation notes, the ability to identify conveniently and securely across the internet for physical persons, companies and devices is a key condition for a seamless Single Market and Single Digital Gateway. GLEIF suggests the eIDAS should be extended to include the link between persons and companies and devices and companies.

As noted in the impact assessment, the Covid-19 pandemic has revealed shortcomings in digital trust services. GLEIF believes the eIDAS review is an excellent opportunity to learn from these events and put in place an adapted eIDAS framework that targets maximum interoperability across borders and engagement with the private sector. A focus on legal entity data sets would help bring transparency to sectors which are heavily impacted by Covid-19 restrictions and are pushing digitization. This includes supply chain management, financial sector customer due diligence protocols, and distribution of government stimuli. A clear requirement for the LEI would anchor the eIDAS framework to a global standard that maximizes the benefits for EU legal entities in Single Digital Gateway and enables non-EU country entities to participate in the extended framework.