bitkom

EBA Draft Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849

2022-March-04

Page 1

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Kevin Hackl
Head of Digital Banking & Financial Services
T +49 30 27576-109
k.hackl@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Introduction

Bitkom welcomes EBA's draft guidance for remote customer onboarding to fulfill Know-Your-Customer (KYC) requirements at this particular point in time. We want to further point out that we appreciate the close alignment with eIDAS, which is regarded to create greater harmonization. With the significant demand for more digital services, increasing applications in AI technology, coupled with the EU's proposal for a secure Digital Identity, EBA's draft is a reminder that assessing the digital ecosystem from a regulatory and technological stance is warranted in order to achieve expedient harmonization across the EU. Amendments to remote KYC onboarding legislation continue to evolve, but there remains fragmentation between national law, which poses risks to security and effects service across Member States. Particularly, Germany's NCA (BaFin) is known for a restrictive use of KYC-compliant remote customer onboarding which poses a severe disadvantage for German financial institutions. The need for maintaining robust security and data privacy provisions is paramount for the digital identity verification ecosystem.

Feedback to EBA

- **Do you have any comments on the section 'Subject matter, scope and definitions'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.**

  According to Bitkom, definitions need further clarification by providing examples and offering procedural guidance for financial institutions.
  Paragraph 9: The current definition of Digital Identity Issuer risks complicating the single market for remote onboarding service providers in the EU. There is a distinction

between an Issuer of a Digital Identity (i.e. eID service providers under eIDAS) and a business providing verification/authentication services for the purposes of onboarding. This distinction should be reflected in the EBA guidelines to avoid any confusion. European legislative tools (including Regulations, Directives, Delegated Acts and Guidelines) should have consistent definitions to avoid fragmentation in the application of rules, and to provide legal certainty to market participants.

- **Do you have any comments on Guideline 4.1 'Internal policies and procedures'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.**

Section 4.1.3 remains unclear in terms of whether the requirements only refer to entities relying on trust services. Paragraph 16 is directly referencing qualified trust providers; the guidelines should also allow for financial service providers to consider service providers that have received certification through a national conformity assessment body under the eIDAS Regulation (which are not considered qualified trust service providers) to still appropriately meet the criteria in paragraph 15.
Service providers having received equivalent certification under the eIDAS Regulation or the AML Directive uphold the same standards. Therefore, they should not have to prove their process requirements through yet another set of criteria. Paragraph 15 should also stipulate that once one Member State recognizes that a service provider meets all the criteria set out in the paragraph mutual recognition across Europe should be applied. Thereby, service providers are not mandated to provide the same proof every time they choose to expand their service to a new marketplace within the EU.

- **Do you have any comments on the Guideline 4.2 'Acquisition of Information'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.**

Evidence collection, in the sense of identification of evidence to accept, could be more stringently defined in the guidelines in order to provide clarity.

- **Do you have any comments on the Guideline 4.3 'Document Authenticity & Integrity'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.**

This section starts with the sentence: "*Where the financial sector operators accept paper copies, photos or scans of paper-based documents in the course of remote customer onboarding without having the possibility to examine the original identification*

document, they should take steps to have sufficient assurance as to the reliability of the copy provided. ***This may include verifying***". Phrases such as "may include" are exactly what leads to differing interpretations of the rules by national competent authorities. We would argue for a risk-based distinction of the various steps, which would set out what steps are required depending on what levels of risk are involved.

- **Do you have any comments on the Guideline 4.4 'Authenticity Checks'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.**

The document is not clear on when a fully automated process based on biometrics is allowed and Paragraph 39 suggests manual check: "Financial sector operators should verify the unambiguous match between the biometric data indicated on the submitted identity document and the customer being onboarded.

Paragraph 42 on insufficient quality: The guidelines should allow for repeated attempts of remote customer onboarding with other pieces of evidence as well as a face-to-face verification via videoconference. Only after repeated attempts and the virtual face-to-face prove unable to alleviate the 'uncertainty and ambiguity' should the customer be required to have a face-to-face interaction in the same physical location.

Photo Quality: paragraph 43(a) requires "absolute clarity" in photographs. We would suggest more precise language, such as "the required properties are captured with the necessary clarity to allow the proper verification of the customer's identity." as is the case in paragraph 44(a).

Liveness detection: paragraph 43(c) appears to require liveness detection verifications as part of any instance of photograph-based onboarding. This is not appropriate as it does not take a technology neutral approach, fails to consider solutions which are widely used in the market and work effectively, and is disproportionate in terms of what it seeks to achieve. As underlined in paragraph, liveness detection should be left for cases where ML/TF risks are higher, rather than a default necessity for all photograph-based onboarding processes.

Paragraph 43(d) on reliable algorithms: it is welcomed that reliable algorithms are allowed for completing verification instead of the need for human verification. Nevertheless, we do still require clarity on what the wording "in the absence of human verification" means. Does this mean that operators can choose AI over humans to verify

without issues, or is this only allowed where humans cannot do so for distinctive reasons? We assume this would be the former, and if so, we would recommend clarifying the passage to avoid misinterpretations on national levels.

Paragraph 47 on waving specific requirements: "*Where financial sector operators resort to digital identity issuers to identify and verify the customer, which are qualified trust services in accordance with Regulation (EU) No 910/2014, or to any other digital identity issuer regulated, recognised, approved or accepted by the relevant national authorities as referred to in Article 13(1)(a) of Directive (EU)2015/849.*"

While the meaning of this sentence is a bit unclear, the likely interpretation is that if qualified trust services, or electronic identification accepted for AML purposes by the national authority, are used, then there is no need to check how these actors carried out the identity proofing.

- **Do you have any comments on the Guideline 4.5 'Digital Identities'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.**

In addition to recognizing qualified trust services, the guidelines (paragraph 48) state that *financial sector operators should use a Digital Identity Issuer with a similar level of assurance as to the level substantial or high as in relation to trust services under Regulation (EU) No 910/2014, which are in particular, similar in relation to reducing substantially the risk of impersonation, misuse or alteration of the identity*. The phrase "in relation to trust services" seems slightly vague here. The reference to the assurance level "substantial" as outlined in eIDAS ((EU) No 910/2014) chapter 2 should be referenced more clearly.

- **Do you have any comments on the Guideline 4.6 'Reliance on third parties and outsourcing'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.**

Regarding the use of digital identities in the onboarding process, presumably including qualified trust services, it is not explicitly stated that this should not be considered as outsourcing.

Requirements in paragraph 56 (a) "necessary steps" do not provide the needed clarity to match national KYC requirements which causes difficulties to rely on TPPs. In general, section 4.6 should incorporate sub-outsourcing to effectively harmonise the EU

outsourcing regime and create further certainty for CDD service providers. This is especially important as tech businesses and startups in the AML space tend to specialize on specific elements of the CDD process.

Conclusion

As stated in the introduction, Bitkom very much welcomes EBA's efforts to further harmonize remote customer onboarding across the EU. Providing a framework that further facilitates the use of digitized solutions of remote customer onboarding is of critical importance to the entire financial industry. Reducing intra-European fragmentation is key to deepen the European financial single market as it not only helps overcome regional disadvantages (e.g. in Germany) but to also supports financial institutions in scaling their businesses across Europe.

Bitkom fully appreciates EBA's draft guidelines that clearly aim to fulfill this goal. However, the guidelines need further refinement for instance with regard to the use of definitions (Subject matter, scope and definitions) as well as more precise language and procedural outlines to eventually overcome national goldplating by NCAs during the implementation.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.