Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 425–433
https://doi.org/10.54941/ahfe1006854

Stakeholder Perspectives on Biometrics-Based Multi-Factor Authentication for eIDAS Levels of Assurance: Insights on Usability, Security, and Privacy

Bian Yang[1,2] and Mads Egil Henriksveen[3]

[1]Norwegian University of Science and Technology (NTNU), Gjøvik, 2815, Norway
[2]Biofy AS, Raufoss, 2830, Norway
[3]Buypass AS, Gjøvik, 2821, Norway

ABSTRACT

Adopting biometrics as an electronic identification (eID) means for online authentication, in addition to its currently popular use for personal device access control, seems a promising solution to achieving both security and convenience of day-to-day online logins. However, the varied approaches to implementing biometrics in MFA may raise different concerns of inclusivity, usability, privacy, and regulatory compliance (*e.g.*, the EU's eIDAS Levels of Assurance *Substantial* and *High*). This study explores how stakeholders (users and experts) perceive biometrics-based Multi-Factor Authentication (MFA), focusing on accessibility, privacy, security, and trustworthiness. Eight key questions guided the work, addressing issues such as remote and mobile biometrics, factors' combination in MFA, biometric data storage, and secret key management, under the context of eIDAS-related standards and guidelines (*e.g.*, BSI TR-03166, ETSI TS 119 461). We surveyed 413 users (Norwegian and English) and interviewed 26 experts across six stakeholder groups: service providers, individual users, academia, eID and biometric technology providers, and authorities / consultants. Results show most users prefer storing biometric data in secure device over cloud services, and oppose shared biometric access (*e.g.*, FaceID) on multi-user devices. Security and privacy were prioritized over convenience by almost two-third of the surveyed participants. Most of them favored MFA combinations adaptive to users' need. For compliance to LoA High, experts emphasized unique device-user pairing, limited shared access, and the need for multiple factors. They also warned of risks from AI-generated fakes and regulatory uncertainty. Overall, the findings confirmed tensions between usability, inclusivity, and privacy, highlighting the need for flexible, transparent, and accessible biometric MFA designs. Future systems, including the EU Digital Identity Wallet, should ensure privacy-preserving biometrics that meet regulatory assurance levels while remaining usable for all, including elderly and disabled users.

Keywords: Biometrics, eIDAS, Multi-factor authentication, Usability, Privacy, Security, Stakeholder perspectives

INTRODUCTION

Electronic identification (eID) means are a key to securing digital interactions. In the European Union, eID is governed by the eIDAS Regulation (EU) No 910/2014, which establishes Levels of Assurance (LoA) to ensure trustworthiness. LoA High, the most stringent level, demands authentication mechanisms to mitigate risks posed by attackers with high attack potential, towards *e.g.*, high-value transactions, such as banking or health data access. Biometrics (fingerprints, facial recognition, iris, *etc.*) offer a promising inherent factor ("who I am") in multi-factor authentication (MFA), enhancing convenience while potentially elevating security beyond traditional knowledge ("what I know," *e.g.*, PIN) or possession ("what I have," *e.g.*, smartcard, one-time-password token) factors. Recent advancements, including eIDAS 2.0's emphasis on the European Digital Identity Wallet (EUDIW) European Commission (2025), show the potential of using biometrics to implement self-sovereign identities. Biometric-enabled remote ID proofing for on-boarding new customers have been increasingly adopted since COVID19. However, enabling biometrics for day-to-day remote authentication as a biometric factor defined under eIDAS raises multifaceted challenges. These include accessibility for vulnerable populations (*e.g.*, elderly or disabled users), privacy concerns under GDPR, and divergent stakeholder interpretations of trustworthiness. Most existing research work related to biometrics and MFA focused on the technical aspects (algorithm, performance testing, *etc.*) but little research have been done to evaluate the feasibility of adopting biometrics to day-to-day authentication use as part of MFA, particularly under the legal context of GDPR and eIDAS. A survey of technological trends in eIDAS-compliant schemes (Sharif et al., 2022) reveals that biometrics primarily serve as PIN alternatives in authentication, predominantly via device-native implementations (*e.g.*, fingerprint or facial unlocking), which ENISA considered insecure (ENISA, 2020). The Qubit HIGH (*Qualifying biometrics-Assisted Authentication towards eIDAS Level of Assurance HIGH*) (Research Council of Norway, 2023) project, funded by the Research Council of Norway (2022-2023), addressed these by fostering mutual understanding among stakeholders towards biometrics' use for authentication compliant with eIDAS LoA High. The project began with eight foundational questions: (1) Can biometrics be used for remote authentication? (2) Is device biometrics a biometric factor under eIDAS? (3) Should biometrics be used on multi-user devices? (4) Can software (*e.g.*, mobile app) be used as a possession factor? (5) Should factors be used in sequence or in parallel for MFA? (6) Is a rich O/S suitable for biometric processing? (7) What is a dynamic authentication parameter for? (8) Should a secret key to authentication be managed locally or remotely?

To find answers to these questions, we took as reference key standards and technical reports:

- Commission Implementing Regulation (EU) 2015/1502 (Specification 1502)
- BSI TR-03159 Part 1: "Security Requirements for eIDAS LoA 'substantial"' (Version 1.0 Draft 2) (2019)

- BSI TR-03166 “Technical Guideline for Biometric Authentication Components in Devices for Authentication” (2021)
- ETSI TS 119 461 v1.1.1 “Technical Specification: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects” (2021)

and reference opinions from the eIDAS Cooperation Network. In addition, questionnaire and interviews were arranged to collect opinions from both the general public and experts with different professional backgrounds. This paper synthesizes questionnaire and interview data from this research, offering guidelines to bridge stakeholder gaps and advance the understanding of the potential of privacy-preserving biometrics for authentication for the future EU Digital Identity Wallet. eIDAS interoperability hinges on harmonizing eID and MFA technologies with GDPR, underscoring the timeliness of this work.

METHODOLOGY

Refinement of Questions

The original eight questions were discussed first within the project’s consortium (Biofy AS, NTNU, Buypass AS, KPMG, KU Leuven), and some of them were found to be too technical for lay audiences, prompting redaction; and a few new questions were added to further probe into end users’ propensity of using biometrics and MFA (see Table 1). Deletions addressed resolved issues (at least achieving common understanding within the consortium), while additions captured more preferences. Some questions were retained only for experts, focusing on technical nuances. This refinement occurred via project meetings and e-mail based discussions, ensuring alignment with eIDAS requirements for LoA Substantial and High. This iterative process considered of the background information about the EUDIW concept under eIDAS 2.0 too.

Data Collection

We employed a two-step methodology: anonymous questionnaires facing the general public for broad input and semi-structured expert interviews for depth. The data collection happened April-June 2023.

Questionnaires were made dual-language (Norwegian/English) via Nettskjema (an anonymous online survey widely used by researchers in Norway) and a private survey company’ service, targeting 413 respondents (301 Norwegian, 112 English) with basic eID experience. The call-for-participation invitation of the English version were posted in various channels (email lists, social media, consortium’s personal connections, *etc.*) so the respondents may have come from outside Norway and Europe. The actual questions were not entirely the same as the redacted questions in Table 1 but further combined and refined to reduce the cognitive burden of participants (shown in Table 2).

Expert interviews (n = 26) spanned six categories: service providers (banks/hospitals, n = 5), end users (n = 4), academics (n = 5), eID providers (n = 3), biometric providers (n = 1), and authorities/consultants (n = 4). To compensate for the lack of intra- and inter-category discussions, the interviews were organized in an asymptotically semi-structured way, *i.e.*, starting with the structured but open-ended (with pre-defined and ordered questions but allowing the interviewees' ramification to relevant topics) method with the first few interviewees, and continuing with the semi-structured interview (without fixed order, allowing greater flexibility and autonomy for interviewees) method with the rest interviewees. However, there is no clear boundary between the two methods' use during this process. These interviews were arranged in sequence, which shared the questionnaire-based survey results and the anonymized prior responses with the next interviewee for an asynchronous cross-pollination. 18 questions based on the survey results were used to probe the experts' opinions on the questions listed in Table 1 but with also new questions on AI impacts, Digital Markets Act (DMA) implications, *etc.*

This approach, while constrained by scheduling, resulted in rich insights, with somewhat methodological rigor through triangulation among document analysis, survey, and interviews.

Table 1: Questions redaction and addition.

Original Question	Redaction/Addition	Rationale
1. Can biometrics be used for remote authentication?	deleted	eID vendors saw it is coming in future especially meeting need from EUDIW. Many users expect it though with privacy concerns.
2. Is device biometrics a biometric factor under eIDAS?	"Two faces to open the same phone?"	Simplified for lay understanding via scenario.
3. Should biometrics be used on multi-user devices?	kept for experts (left out from the general public)	Whether a device/app unlocked by biometrics held by more than one users is regarded as a possession factor seems too abstract for a layperson to understand.
4. Can software (*e.g.*, mobile app) be used as a possession factor?	kept for experts (left out from the general public)	The pros and cons of using hardware and software possession factors seems difficult for a layperson to understand.
5. Should factors be used in sequence or in parallel for MFA?	"One, two, or three factors?"	Redacted to a virtual example to facilitate a layperson to understand.

Continued

Table 1: Continued

Original Question	Redaction/Addition	Rationale
6. Is a rich O/S suitable for biometric processing?	"Where is my biometric data?"	Redacted to asking for preference instead of judgement
7. What is a dynamic authentication parameter for?	deleted	Addressed by LoA Guidance/Specification 1502; interpreted by eID suppliers.
8. Should a secret key to authentication be managed locally or remotely?	kept for experts (left out from the general public)	Too complex for a layperson to understand trade-offs and trustworthiness
New question	"Accuracy, convenience, or security/privacy?"	To measure priorities
New question	"Biometrics vs. PIN?"	To gauge views on re-authentication
new question	"Which two factors?"	To assess propensity using biometric in MFA
New question	"Which use cases?"	To collect contextual preferences
New question	Demographics (*e.g.*, age, eID experience)	To know respondents' demographic background

Table 2: Comparison of questionnaire answers (% respondents per option; only most voted 1 or 2 options are included).

Question/Key Finding	Option (Shortened)	English (%)	Norwegian (%)
Q1. Two faces to open one phone Key finding: Oppose unless app-specific	Should not be allowed Allow only limited apps	51 31	60 20
Q2. Where is biometric data stored Key finding: User's hardware preferred over cloud	User's secure hardware Trusted cloud	70 46	51 24
Q3. Priority in biometrics Key finding: Security/privacy > convenience	Security/privacy most important Accuracy most important	65 41	61 34
Q4. Biometrics vs PIN Key finding: equivalent, biometrics mainly for convenience	Two-factor combination Biometrics mainly for convenience	60 38	58 32
Q5. Preferred factor pair Key finding: highly dependent on use case; knowledge + biometric slightly more preferred	Depends on use case Knowledge + biometrics	41 28	24 35
Q6. Attitude toward biometrics	Positive/Very positive	69	53
Q7. Future popularity	Increasingly popular	63	38

DATA ANALYSIS

Questionnaire

Without losing fidelity, we summarize the questionnaire answers' statistics as in Table 2, where only the most voted answers 1 or 2 options are included. Key findings are also summarized. Survey data highlighted privacy as a paramount need. In Q2 (biometric storage), 50–70% favored personal secure hardware (*e.g.*, code chips) over software (PCs) or clouds (*e.g.*, iCloud), due to leakage fears. This is aligned with GDPR's defining biometric data as sensitive data. Q3 showed 60–65% prioritizing security/privacy over accuracy/convenience, with only 20% favoring usability alone. This echoes the trend we observed in recent years users desire hardware-bound biometrics for trust. On MFA preferences (Q4), 60% equated biometrics with PIN for re-authentication, and Q5 revealed balanced factor pairings (possession + knowledge: 28–34%; biometrics + possession: 16–20%; knowledge + biometrics: 28–35%). Attitudes (Q6) were neutral-positive (26–39%), and 23–46% predicted biometrics' future popularity (Q7) same as today, and 38–63% predicted it to be more popular.

Expert Interviews

Interviews revealed consensus on biometrics' LoA High potential but admitted practical barriers. Service providers (banks/hospitals) endorsed unique possession factors and hybrid MFA, rejecting shared devices; hospitals sought elderly-user friendly options. Academics highlighted legal hurdles in delegation, advocating in-parallel MFA (all factors visible to the authentication server) for security over in-sequence MFA which is user-friendly but weaker in security. eID providers stressed secure hardware for LoA High, and FIDO2 passkeys were critiqued for copy risks if they are allowed to be exportable and not device-bound anymore. Biometric providers noted AI deepfakes as evolving threats, favoring an in-parallel authentication. Authority and consultancy emphasized that the risks associated with context of authentication matter over merely counting how many factors. It is a cross-sector concern towards generative AI which was thought to be able to facilitate attacks. EU Digital Markets Act is pushing for open secure hardware (*e.g.*, Apple secure enclave), which can boost innovation but opening the secure hardware can risk security too. Software possession is permissible but hardware superior for user-controlled devices. Market inhibitors for adopting biometrics for authentication include regulatory ambiguity and interoperability fragmentation. Self-sovereign identities (*e.g.*, EUDIW) open a new market for biometrics.

DISCUSSION

Balancing Usability and Assurance

Results from the questionnaire survey demonstrate that while biometric authentication offers convenience, users consistently prioritize security and privacy over ease of use when biometrics is supposed to be used. This aligns with our findings in the interviews where most respondents associated biometrics with high-assurance contexts such as banking and healthcare rather than casual applications. Both expert and user perspectives revealed that trust in biometric MFA depends heavily on transparent data handling (*e.g.*, visibility of biometric data processing to authentication server) and the ability to manage consent dynamically.

Norwegian respondents exhibited a more conservative stance, reflecting the country's strong culture of data protection and reliance on state-backed eID systems like BankID. International respondents were generally more open to flexible configurations and commercial service integration, suggesting cultural or regulatory confidence differences. Experts across all categories emphasized that biometric MFA must not undermine inclusivity; fallback methods like PINs or delegated access are essential for users with disabilities or cognitive impairments.

Trust, Privacy, and Factor Separation

Biometric data, being an inherent factor, cannot alone meet the LoA Substantial or High requirements. The findings from interviews underline the crucial role of separation of authentication factors in achieving eIDAS LoA High. Most opinions prefer two factors to be authenticated in parallel instead of in sequence for security consideration, while the latter seems more user-friendly and possibly more cost-efficient. Experts stressed that the possession factor, which is often represented by a secure personal device, should be cryptographically unique and tamper resistant. Many advocated that biometric comparisons should happen locally within a Trusted Execution Environment (TEE) or Secure Enclave, minimizing risks of template leakage.

The surveys further support this preference: a majority of both international and Norwegian participants favored local storage over cloud-based options. This preference reflects increasing awareness of privacy and requirement of protecting biometric data as sensitive data under GDPR. On the other hand, experts warned that current legislative ambiguities, particularly around remote biometric verification, could stall innovation unless clear technical standards emerge.

AI-Driven Threats and Regulatory Implications

AI-generated forgeries pose a direct challenge to the trustworthiness of biometric authentication. The respondents highlighted their growing concern over deepfakes and synthetic identities capable of mimicking facial or voice biometric traits. Experts recommended continuous liveness detection, multimodal biometrics, and dynamic challenge-response verification to mitigate these threats. Additionally, audit mechanisms must ensure algorithmic transparency and fairness, preventing discriminatory outcomes across demographic groups.

From a regulatory standpoint, the eIDAS 2.0 framework and the upcoming European Digital Identity Wallet will require stricter auditability and risk assessment for biometric systems. The EU Digital Markets Act (DMA) may indirectly influence these developments by mandating controlled access to secure hardware features in mobile devices, potentially democratizing high-assurance MFA. However, experts noted that the coexistence of multiple national certification schemes could lead to fragmentation unless harmonized under EU-wide conformity standards.

Inclusivity and Delegation

Inclusivity remains a persistent challenge. In the questionnaire-based surveys, respondents expressed concern about systems that might exclude elderly or disabled users. Expert interviews, especially from healthcare and public-sector participants, proposed delegated access models that allow trusted individuals to authenticate on behalf of others under consent-based protocols. Such flexibility aligns with the principles of universal design and the EU's accessibility directives. However, this delegation must be diligently audited to maintain trust.

CONCLUSION

This paper explores stakeholder perspectives on biometrics-based multi-factor authentication (MFA) for achieving high assurance under the EU's eIDAS regulation. Drawing on data from two public surveys, one in English with international respondents ($n = 112$) and one in Norwegian ($n = 301$), and 26 expert interviews across six stakeholder groups, the study examines how users and professionals interpret usability, security, and privacy trade-offs in biometric authentication.

Findings show broad agreement that biometrics improve user convenience but cannot alone meet eIDAS Level of Assurance (LoA) Substantial or High. Respondents prioritize privacy and security over convenience, though deeming biometrics more as a convenient factor, preferring biometric comparison and data storage in secure device hardware controlled by users rather than in the cloud. Norwegian respondents were more cautious and regulation-focused, while international respondents expressed greater trust in technology and optimism toward biometric adoption. Experts emphasized that high assurance requires strict factor separation, hardware-based possession factor, and on-device biometric data processing to prevent biometric information exposure.

Emerging challenges include AI-generated identity forgeries, uneven regulatory interpretation, and accessibility barriers for older or disabled users. Experts proposed adaptive and delegated authentication models to ensure inclusivity without compromising security. Overall, the study highlights the need for transparent, privacy-preserving, and context-aware MFA solutions. Future eIDAS-compliant systems such as the European Digital Identity Wallet should integrate biometrics as part of layered, user-centric trust architectures that ensure both strong assurance and universal accessibility.

ACKNOWLEDGMENT

This work was fully funded by the Research Council of Norway through the project "Qualifying biometrics-Assisted Authentication towards eIDAS Level of Assurance HIGH (Qubit HIGH)" (project number 337697), partially funded by the project “Leveraging Security and Privacy Technologies for Inclusive eID and Access Control Services (IncluDe)” (project number 349943) and the project “Application-Level Continuous Authentication (AppLeCAt)” (project number 357676).

REFERENCES

European Commission (2025) EU Digital Identity Wallet Home. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU%2BDigital%2BIdentity%2BWallet%2BHome (accessed 31.10.2025).

ENISA. eIDAS Compliant eID Solutions - Security Considerations and the Role of ENISA. 2020.

Research Council of Norway (2023). Qualifying biometrics-Assisted Authentication towards eIDAS Level of Assurance HIGH (Qubit HIGH). FORNY20-FORNY2020, Kommersialiseringsprosjekt / Kvalifisering. https://prosjektbanken.forskningsradet.no/project/FORISS/337697?Kilde=FORISS&distribution=Ar&chart=bar&calcType=funding&Sprak=no&sortBy=score&sortOrder=desc&resultCount=30&offset=0&Fritekst=Qualifying\protect$\relax+$biometrics-Assisted\protect$\relax+$Authentication (accessed 31.10.2025).

Sharif, A.; Ranzi, M.; Carbone, R.; Sciarretta, G.; Marino, F. A.; Ranise, S. (2022) The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Appl. Sci.* 2022, *12*, 12679. https://doi.org/10.3390/app122412679.