Technology and Regulation

special issue: security in the digital age

Attribute-based signatures and eIDAS 2.0

Author(s)	Yong Yong Hu
Contact	yongyong.hu@ru.nl
Affiliation(s)	Yong Yong Hu is a PhD candidate at the Radboud Business Law Institute of Radboud University, Nijmegen, the Netherlands: Trainee judge at the Rotterdam District Court.

Keywords	Digital authentication; eIDAS 2.0; electronic signatures; European Digital Identity Wallets; attributes; GDPR; digital identities; trust services; attribute-based authentication; attribute-based signatures.
Published	Published: 31 Mar 2026
Citation	Yong Yong Hu, Attribute-based signatures and eIDAS 2.0, Technology and Regulation, 2026, 44-56 • 10.71265/okjh4e70 • ISSN: 2666-139X

Abstract

Digital authentication and electronic signatures are essential for reliable digital verification of identities in the digital environment. With the introduction of European Digital Identity Wallets under eIDAS 2.0, there has been a shift in the use of trust services. In this contribution, I examine whether eIDAS 2.0 facilitates the use of privacy-friendly trust services, in particular attribute-based authentication (ABA) and attribute-based signatures (ABS). ABA and ABS provide benefits such as modular identities and role-based signing, offering greater flexibility compared to traditional trust services. The analysis shows the difference between authentication and signing, revealing that eIDAS 2.0 only facilitates ABA through the European wallets, but not yet ABS. The article concludes by discussing the remaining legal challenges that may impede the full realisation of privacy-friendly trust services.

1. Introduction

Digital identities are indispensable in the current digitalised society. They enable natural and legal persons to authenticate themselves online.[1] Reliable digital verification of identities can mitigate the risk of identity theft and other forms of abuse. In addition, better surveillance can be carried out to track illegal activities.[2]

[1] Marloes de Koning, 'Europese digitale identiteit is straks niet veilig genoeg, waarschuwen experts' *NRC* (Amsterdam, 22 December 2024).

[2] When an unauthorised person attempts to log in, a relying party can issue automatic warnings and block accounts.

Therefore, the European Commission introduced the eIDAS Regulation (eIDAS 1.0) in 2014 to improve the internal market by providing a harmonised framework for the use of digital identities and trust services, including electronic signatures.[3] Electronic signatures are important because they not only provide proof of agreement with the content of a contract but also ensure a verifiable link between the signature and the signatory.[4] However, national digital identification systems were not accessible to the entire society, were limited to online government services and were not easy to use in other Member States (only 14% of public service providers accepted digital identification systems from another country).[5]

In order to increase the reliability of authentication for cross-border electronic transactions, the European Commission revised the regulatory framework for electronic identity solutions. The revised regulation (eIDAS 2.0) entered into force on 20 May 2024.[6] With this revision, the legislator wants to make major changes to eIDAS 1.0 and has amended the original regulation and supplemented it with new provisions. In this article, I always use the article numbering of the consolidated version of the regulation.[7] When I refer to the recitals, I am referring to the recitals in the revised regulation.

While eIDAS 1.0 did not facilitate authentication or signing using attributes, eIDAS 2.0 introduces the European Digital Identity Wallets and the associated possibility of using 'attributes' to verify an individual's identity (authentication). The European Digital Identity Wallet is an electronic identification means that enables the user to store, manage, and validate (among other things) personal identification data and electronic attestations of attributes in a user-friendly and transparent manner.[8]

An attribute is a piece of personal information that partially describes a characteristic of an individual.[9] Examples include a residential address, citizen service number or age. Attribute-based authentication (ABA) has the advantage of enabling contextual authentication. For example, if a user only needs to share an age limit to buy alcohol online, ABA allows them to share only an attribute with an age limit 'over 18' with the relying party.[10] This also contributes to data minimisation, as no more personal data is shared than necessary.

The wallets also allow users[11] to create qualified electronic signatures. As with eIDAS 1.0, this can still be done using traditional certificate-based electronic signatures (CBS), as these meet the requirement for a qualified certificate. A qualified certificate links the electronic signature to a natural person and always contains a standard set of (personal) data.[12] However, eIDAS 2.0 does not specify whether it is also possible to create qualified electronic signatures using different attributes in the wallet.

Facilitating such attribute-based signatures (ABS) has several advantages (see Section 2.2.2 for more details). First and foremost, ABS make it possible to share additional information in a reliable and verifiable manner. A user can sign with specific attributes, such as their name, age and/or professional accreditation.

[3] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73 (eIDAS Regulation).

[4] Bart Jacobs, 'The authenticity crisis' (2024) 53 Computer Law & Security Review 105962

[5] European Commission, 'European Digital Identity'https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

[6] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) 910/2014 as regards the establishment of a European Digital Identity Framework [2024] OJ L1183.

[7] See consolidated version, Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market [2014] OJ L257/73 (consolidated version 18 October 2024).

[8] eIDAS 2.0 (n6), arts 3(42), 5a(4).

[9] Elisa Bertino and Kenji Takahashi, *Identity Management: Concepts, Technologies, and Systems* (Artech House 2011) 22.

[10] eIDAS 2.0 (n6), art 3(6) defines a relying party as a natural or legal person that relies upon electronic identification means, including European digital identity wallets.

[11] eIDAS 2.0 (n6), art 3(15) defines the user as a natural or legal person who uses a trust service or the electronic identification means provided.

[12] eIDAS 2.0 (n6), art 3(15) and Annex I.

This allows the user to sign in different roles, such as in their profession as a medical professional or as a consumer, without sharing unnecessary personal data.[13]

This article focuses on the following question: to what extent does eIDAS 2.0 facilitate the utilization of the possibilities and advantages of attribute-based authentication and signatures? To answer this question, I will first describe what ABA and ABS are in section 2. In that section, I also examine the revisions made in eIDAS 2.0 regarding attributes, electronic signatures and European wallets. In section 3, I examine whether the possibilities of ABA and ABS can be exploited with the revision of the eIDAS Regulation and what the possible limitations are. Finally, I end with a conclusion in section 4.

2. Attribute-based authentication and signing

The following subsections first approach authentication from a technical perspective, followed by the characteristics of ABA as a privacy-friendly option for authentication (Section 2.1). This is followed by an analysis of digital signatures and the characteristics of privacy-friendly ABS (Section 2.2). The section concludes with the objectives of European Wallets, which try to enable both ABA and ABS to support secure and privacy-preserving digital identity use (Section 2.3).

2.1 Authentication

2.1.1 Digital authentication

Authentication is the process whereby the identity of the user is verified by a relying party. Authentication is about proving who (or what) you are. Commonly used authentication methods include keycards (something you have), passwords (something you know) or biometrics (something you are). Authentication usually takes place using electronic identification means (eID), such as a DigiD or iDIN. The strength of the authentication is important for the levels of reliability that can be offered.[14] Authentication is temporary and only applies for the duration of a session, which means that authentication does not offer permanent proof.[15] Authentication can also take place using a wallet.

A wallet is software that allows various attributes (such as address, age, vaccination status) to be securely stored, managed and shared.[16] The wallet functions, for example, as a mobile application that allows users to easily store the desired attributes in their wallet on their phone and select them for authentication (or signing).[17]

To ensure user privacy, various technologies, such as zero-knowledge proof (ZKP), can be integrated into the wallet.[18] ZKP is a cryptographic protocol that allows a person to be authenticated, whereby the proof is provided in a signed form that cannot be reused with a signature by another person.[19] A user

[13] When purchasing alcohol online, for example, it is sufficient to sign with the age attribute “over 18” without sharing your exact age. Yong Yong Hu and others, ‘Attribuut-gebaseerde elektronische handtekeningen en de eIDAS-verordening’ in Pieter TJ Wolters and Ruud M Hermans (eds), *Digitalisering en conflictoplossing*, Serie Onderneming en Recht (Wolters Kluwer 2021) 308–309.

[14] eIDAS 2.0 (n6), art 8 sets out the different levels of assurance for electronic identification means.

[15] Cf electronic signatures that can guarantee non-repudiation. See also Section 2.1.2.

[16] Zahra E Ansaroudi and others, ‘Control Is Nothing Without Trust: A First Look into Digital Identity Wallet Trends’ (2023) 114 International Federation for Information Processing 117–120; Blaz Podgorelec and others, ‘What Is a (Digital) Identity Wallet? A Systematic Literature Review’ in *Proceedings of the IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (IEEE 2022) 814–816.

[17] Julián Inza, ‘The European Digital Identity Wallet as Defined in the eIDAS 2 Regulation’ in Carmen Pastor Sempere (ed), *Governance and Control of Data and Digital Economy in the European Single Market* (Law, Governance and Technology Series, Springer 2025) 439–442. See section 2.3 on signing.

[18] Jitendra Kurmi and Ankur Sodhi, ‘A survey of zero-knowledge proof for authentication’ (2015) 5 *IJARCSSE* 494-495; Adwait Pathak and others, ‘Secure authentication using zero knowledge proof’ (Asian Conference on Innovation in Technology (ASIANCON), August 2021), 1-8, doi: 10.1109/ASIANCON51346.2021.9544807.

[19] One party (user) can prove to another party (relying party) that a certain statement is true, without revealing the data on which the statement is based. ZKP has the advantage that the user does not have to share the data with the relying party, but the relying party cannot be misled by the user or act as the user towards a third party.

who wants to access an online platform can use cryptographic proof to demonstrate that they are over 15 years of age without revealing their exact date of birth. They can use their cryptographic proof to prove to the online platform that the attribute is valid, that it comes from a trusted issuer, and that they meet the age requirement.

Three actors are important for the wallet ecosystem to function properly.[20] Firstly, wallet providers must build the wallets for users and provide technical support to users and relying parties along the way. Secondly, issuers must issue reliable attributes, such as a diploma or driving licence.[21] Issuers must also issue accompanying certificates to guarantee the reliability of the attributes.[22] Finally, service providers (the relying parties) rely on the information from the wallets to complete user authentication for the performance of their services. An example is a car rental company that needs to verify whether the person seeking to rent a car holds a valid driving licence.

2.1.2 Characteristics of attribute-based authentication

An attribute is a characteristic, quality or right of a natural or legal person.[23] Common attributes include age, address and professional qualifications. Attributes can be authenticated by means of an attestation in electronic format.[24] In short, an attestation is a statement by entity X that person Y possesses attribute Z. For example, the municipality declaring that the user has a specific citizen identification number, or a university declaring that the person is studying at that university. The electronic attestations of attributes in the wallets can be issued or validated by (qualified) trust service providers, such as government agencies or recognised private institutions, via a digital signature.[25]

An attribute offers no certainty if it is unclear whether the electronic attestation is reliable. Name verification based on the membership database of the local sports club is less reliable than verification based on official registration with the municipality. It is therefore important that attestations are from a reliable source (as is the case with electronic signatures and eID).

The entire infrastructure for managing, issuing and verifying attributes is referred to as an attribute system.[26] Both ABA and ABS are part of an attribute system. This means that the characteristics of an attribute system as described below also apply to ABS.[27]

One of the most important characteristics of an attribute system is modular identity. Instead of presenting a full identity each time, users disclose only certain characteristics about themselves, depending on the application, without sharing more personal data than necessary. This offers flexibility and the possibility of data minimisation.

An additional feature of ABA is that attributes can be stored decentralised, allowing users to retain control over their own personal data. Depending on the type of cryptography and what the application passes on to the application issuer, a central authority cannot see when or for what purpose the attributes are used.[28] For example, the central authority will not be able to see when a user logs into a gambling website several times.

[20] The user is actually the fourth party. Ansaroudi (n16) 113-115; Podgorelec (n16) 809.

[21] Unlike CBS, the CA does not play a role in the registration and issuance phase.

[22] See Section 2.1.2 for an explanation of attestations.

[23] eIDAS 2.0 (n6), art 3(43); eIDAS 2.0 (n6), Annex VI also provides a minimum list of attributes; See also Hu et al (n 11) 296-298; eIDAS 2.0 (n6), recitals 59 and 15 also stipulates that it must be technically possible for the user to selectively provide attributes.

[24] ibid, art 3(44). The attestation is essentially a collection of signed hashes, whereby the preimages (data entered into a hash function to calculate a unique hash) are made public by the service provider in order to verify the authenticity of the data.

[25] ibid, recital 55 and arts 3(16)(g), 3(16)(h).

[26] See Section 2.2.2 for an explanation of ABS.

[27] Cf. Section 2.2.2.

[28] Tatsuaki Okamoto and Katsuyuki Takashima, 'Decentralized attribute-based signatures' in Kaoru Kurosawa (ed), *Public-Key Cryptography – PKC 2013*, Lecture Notes in Computer Science 7778 (Springer 2013) 125–142.

2.2 Electronic signatures

2.2.1 Digital signatures

From a technical perspective, a digital[29] signature is a cryptographic construct that links a message in electronic form to the signer.[30] The digital signature is an attachment to the message. To protect messages against forgery, manipulation and denial, signing is often done using asymmetric cryptography. This means that only the owner of the private key can perform the signing. The user signs the hash value (a unique code representing the content of the message) with their private key. Anyone can then verify the digital signature using the user's public key, which is linked to the private key.[31] In the accompanying public key certificate, the certificate authority (CA) confirms to the relying party that the key pair used for the signature belongs to the user. To make signing with attributes practical, a wallet can also be used.[32]

When the digital signature is valid, three elements are guaranteed. Firstly, integrity: the message has not been altered since it was signed. Secondly, authenticity: the message originates from the owner of the private key. And finally, non-repudiation: because the message can only originate from the owner of the private key and has not been altered, the user cannot deny that they signed the message.[33]

The following example illustrates this. A doctor signs a prescription using a digital signature. A relying party, usually a pharmacy, wants to know whether the message is reliable. If the signature is valid, it is certain that the medicines are being prescribed to the right persons (integrity), that the prescription has been signed by an authorised doctor (authenticity) and that the doctor's identity is established so that they can be held responsible in the event of a medical error (non-repudiation).

2.2.2 Characteristics of attribute-based digital signatures

ABS are signatures in which one or more attributes of the user are included in the attachment to the message in electronic form in such a way that their validity can be verified. They thus make it possible to share specific information about the signatory. This gives the relying party certainty about the characteristics of the signatory.[34]

The characteristics of ABS are illustrated by the following five use cases[35]:
Use case I: only (full) name as attribute
Use case II: two attributes – name and registration number
Use case III: name and gender or age as attributes
Use case IV: a non-identifying attribute, such as “over 18”
Use case V: a pseudonym as attribute

For the first use cases, let's take the same example in which a doctor has digitally signed a prescription, and the pharmacy wants to know whether the signature is genuine. We assume that integrity is satisfied in all use cases, i.e. that the medicines are prescribed to the right persons. We are only looking at authenticity and non-repudiation.

In the first use case, the doctor signs the prescription with only a (full) name as an attribute. However, authenticity and non-repudiation are not guaranteed, as there may be other persons with the same name. The name alone does not make it clear that the user is a licensed doctor.

[29] A digital signature is a technical term that overlaps with the legal term ‘electronic signature’. However, an electronic signature does not necessarily offer the same guarantees. See also Hu (n13) 294.

[30] Hu (n13), 298-299.

[31] See also Hu (n13), 298-301.

[32] See Section 2.1.1.

[33] Khaled S Mohamed, ‘Cryptography Concepts: Integrity, Authentication, Availability, Access Control, and Non-repudiation’ in Khaled S Mohamed (ed), *New Frontiers in Cryptography* (Springer 2020) 41–63.

[34] See also Hu (n13), 298-301.

[35] For a detailed explanation of the use cases, see Hu (n13), 306-312.

If, in addition to her (full) name, the doctor was to use her (unique) registration number from the BIG register[36] to sign, the authenticity of the message's content could be guaranteed. In this second use case, the relying party can verify the doctor's authority in the register (authenticity) and the doctor's identity is also established by the unique registration number (non-repudiation).

Outside her professional environment, the doctor can also use a digital signature in her private life, using only her name and her gender or age. For example, if the doctor visits an online liquor store or participates in a sports club where gender verification may be important. In such cases, it is not necessary to share her professional accreditation. The first three use cases illustrate one of the most important features of ABS: facilitating role-based digital signatures and contextuality. A medical professional can sign in their role as a healthcare provider without actually revealing their identity. This can be important, for example, in some cases when the healthcare provider requests the compulsory admission of a patient, as the provider may fear possible retaliation.[37]

Regarding data minimisation, the user may also decide to sign using only a non-identifying attribute, such as age. This may be important, for example, when verifying age to use social media or a chat website. The user can prove that they are of the appropriate age for social media use (authenticity) with their date of birth or a certain age limit ("over 18"). A non-identifying attribute such as "over 18" is not exclusive. In the context of a chat website, this means that access can be granted on the basis of cryptographic proof of the attribute "over 18" without the user having to reveal their full identity. This is not always necessary in the context of social media either: it is also possible to be active under a pseudonym.

At the same time, there is also a risk of traceability with non-identifying attributes. If a specific user always uses the same key pair to access the chat website, relying parties can link the signatures to each other and trace them back to the user. ABS can offer the possibility of using a unique key pair for each signature. This prevents linking.[38] ABS can thus achieve what is known as "multi-show unlinkability".[39] The last use case involves the use of a pseudonym as an attribute. For example, an activist wants to operate online and on social media without revealing his real identity. The activist can then use a pseudonym to shield their identity for fear of retaliation. With a pseudonym, they can still demonstrate that the messages on the various online platforms and other online channels were sent by the same person. This allows them to build a reputation, which strengthens their credibility.

With pseudonyms, it is of course important that a user cannot be identified on the basis of different attributes of the same user (user unlinkability).[40] Suppose that a user shares a pseudonym during the first interaction and his or her name during the second interaction. In that case, it should not be possible for the relying party to determine that it is the same user. ABS can achieve this user unlinkability by using a different key pair for each attribute. User unlinkability is therefore less extensive than the multi-show unlinkability discussed above, where the different uses of individual attributes must also be unlinkable.

As the use cases show, ABS can offer both security and privacy benefits. They facilitate modular and role-based identity, signing with a non-identifying attribute or pseudonym, and various forms of unlinkability.

[36] The BIG register is an online and public registry in the Netherlands for healthcare professionals. It shows a healthcare provider's qualifications and confirms that they are entitled to practice their profession.

[37] See, Wet verplichte geestelijke gezondheidszorg [Compulsory Mental Healthcare Act] (Wvggz), ch 3.

[38] Hu (n13) 299-301; Brinda Hampiholi and others, 'Towards practical attribute-based signatures' in Rajat S. Chakraborty and others (eds), *Security, Privacy, and Applied Cryptography Engineering* (Springer 2015) 310-328; Hemanta K. Maji and others, 'Attribute-based signatures' in A. Kiayias and others (eds) *Topics in cryptology* (Springer 2011) 376-392; Hemanta K. Maji and others, 'Attribute-based signatures: Achieving attribute-privacy and collusion-resistance' (2008) *IACR Cryptology ePrint Archive* 328.

[39] See also C Baum and others, 'Cryptographers' feedback on the EU Digital Identity's ARF' (2024)https://www.mayrhofer.eu.org/publication/eudiw-cryptographers-statement-2024/, 4–5.

[40] Ali E. Kaafarani and others, 'Attribute-based signatures with user-controlled linkability', in: Dimitris Gritzalis and others (eds), Cryptology and Network Security(Springer 2014), 256-269.

2.3 Objectives of European wallets

eIDAS 2.0 introduces the European wallet with the primary purpose to make trust services available to all European citizens. These services must also be usable for access to a wide range of public and private services.[41] For this purpose, it must also be possible to use attributes (Section 2.3.1). Moreover, the European wallet does not concern electronic authentication alone but must also make it possible to create qualified electronic signatures (Section 2.3.2).

2.3.1 Access to online services

Under eIDAS 1.0, users could not authenticate themselves using separate attributes, as authentication was primarily aimed at identifying natural or legal persons through electronic identification means.[42] With the introduction of eIDAS 2.0, the European Digital Identity wallet was established, enabling the use of ABA.

When a user wishes to access public or private services, they can (selectively) display attributes such as university degrees and driving licences.[43] For example, a user could request the attribute for their degree obtained in the Netherlands from the governmental organisation DUO and add it to their wallet. If they then wish to pursue further education in France and the French educational institution (relying party) requests proof of their degree obtained in the Netherlands, they can demonstrate this by showing the 'degree' attribute in their European wallet to the French educational institution.[44] By authenticating themselves with separate attributes, users have more control over which personal data they want to share with the relying party.[45]

Relying parties that want to use European wallets for user authentication are required to register. The registration makes it easier for Member States to check the legitimacy of online activities by relying parties.[46] When registering, relying parties must also indicate what data they want to collect and the reason behind the request.[47] Relying parties may not request data from users other than that specified in the relying party's register.[48] To protect users from unnecessary sharing of information, the underlying technology of the wallet must inform users if a relying party requests more information than is permitted.[49]

eIDAS 2.0 also includes a framework for the reliability of electronic attestations. Qualified electronic attestations are the most reliable, as these attestations must be issued by a qualified trust service provider[50] and must meet the requirements of Annex V.[51] Digidentity B.V. and the Ministry of Defence are examples of qualified trust service providers in the Netherlands.[52] Annex V of eIDAS 2.0 requires, among other things, that the qualified attestation be identified as such and that it contains information about the qualified provider. The qualified attestation also includes the period of validity, the unique identity code, the qualified electronic signature and the available location. Apart from the requirements in Annex V, there are no other mandatory requirements.[53]

[41] eIDAS 2.0 (n6), recitals 7, 8, 19 and arts 2(1), 2(42), 5a.

[42] eIDAS 1.0 (n3), arts 3(2), 3(5).

[43] eIDAS 2.0 (n6), recital 7 and art 5a(4)(a).

[44] ibid, see also recital 19 for the importance of authentication in the healthcare sector.

[45] ibid, recitals 13, 19 and art 5a(14).

[46] ibid, recital 17 and art 5b(1).

[47] ibid, art 5b(2)(c).

[48] eIDAS 2.0 (n6), art 5b(3); Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets [2024] OJ L, 2024/2979, 29.11.2024, recital 14.

[49] Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties [2025] OJ L, 2025/848, 7.5.2025, recital 10 and art 8(2)(d).

[50] eIDAS 2.0 (n6), arts 3(20), 24.

[51] ibid, art 3(45).

[52] See 'Trusted List Browser' (European Commission) https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/NL accessed 12 June 2025. In the Netherlands, qualified trust service providers are certified by the Rijksinspectie Digitale Infrastructuur [Dutch Authority for Digital Infrastructure].

[53] eIDAS 2.0 (n6), arts 45d(1), 45d(3).

Attestations may also be issued by a public authority who will be responsible for a register or a system.[54] To this end, the attestation must comply with the requirements of Article 45f and annex VII.[55] Annex VII and Annex V are largely similar, as they impose the same requirements on attribute attestations. An attestation of attributes issued by a public authority who will be responsible for an authentic source[56] in one Member State shall be recognised in all Member States as an attestation by a public authority.[57]

Both qualified electronic attestations and attestations issued by a public authority have the same legal effect as a legally issued paper attestation.[58] Given the high reliability requirements, relying parties seeking certainty are advised to accept only attributes issued by means of qualified attestations.

The use of European wallets is voluntary for citizens.[59] Users must also be able to authenticate themselves in another manner and thus gain access to the services. In some cases, however, private relying parties are obliged to accept the use of European wallets.[60] This obligation exists if the parties are required by EU or national law to use strong user authentication[61] for online identification or if such user authentication is required by a contractual obligation. According to Article 5f(2) of eIDAS 2.0, this may apply, for example, in sectors such as transport, energy, banking, financial services, social security, healthcare, drinking water supply, postal services, digital infrastructure, education or telecommunications.

This obligation also applies to very large online platforms (VLOPs)[62] when they require user authentication for access to online services. They must facilitate the use of European wallets if the user requests it.[63] VLOPs must comply with the principle of minimal data processing and accept pseudonyms chosen by users.[64] This obligation for online platforms helps to mitigate the risk of fraud and, in principle, contributes to a high level of data protection.[65]

Users must also be able to authenticate themselves to relying parties in offline mode (without a network connection).[66] This can be achieved with wallets by storing attributes on the device itself.[67] Offline authentication is important in some sectors, for example when there is no network connection in the healthcare sector, where e-prescriptions with QR codes are frequently used.[68] In the event of malfunctions or in remote locations, for example, the dispensing of medication must be able to continue uninterrupted.

A European wallet must also offer the possibility to generate pseudonyms, encrypt them and store them locally.[69] When identification is not required, a relying party cannot refuse the use of pseudonyms.[70] This also applies to access to VLOPs.[71] When a pseudonym is used, this must also be clearly indicated on the attested attributes.[72]

[54] ibid, arts 3(46), 3(47).

[55] ibid, art 45f(1).

[56] An authentic source is the official system that provides the 'truth' for a given attribute, and attestations deriving from it are considered trustworthy under eIDAS 2.0. For example, the municipality is an authentic source for the user's residential address.

[57] eIDAS 2.0 (n6), art 45b(3).

[58] ibid, art 45b(2).

[59] ibid, art 5a(15).

[60] ibid, recital 56 and art 5f(2). Strong user authentication may also be required by contractual obligation.

[61] Strong user authentication is authentication based on at least two authentication factors (two-factor authentication), either something you know (password), something you possess (keycards) or something you are (biometrics); see also eIDAS 2.0 (n6), art 3(51) and Hu (n13) 295-296; The strength of the authentication is relevant to the assurance levels that can be provided, see eIDAS 2.0 (n6), art 5a(5)(d) which stipulates that European wallets must meet the assurance level high.

[62] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC [2022] OJ L277/1 (Digital Services Act), art 33.

[63] eIDAS 2.0 (n6), art 5f(3).

[64] ibid, recital 57.

[65] ibid.

[66] ibid, recital 19 and arts 3(57), 5a(4)(a), 5a(4)(b).

[67] The attributes are not stored on a central server or in the cloud (decentralised architecture).

[68] eIDAS 2.0 (n6), recital 19.

[69] ibid, recital 22 and art 5a(4)(b).

[70] ibid, recitals 19, 22, 60 and art 5b(9).

[71] ibid, recital 57.

[72] ibid, Annex V(c) and Annex VII(c).

2.3.2 To digitally sign

The European wallet is not only intended for electronic authentication, but must also enable qualified electronic signatures to be created. This should be free of charge, but Member States may derogate from this rule when used for professional purposes.[73]

Despite the introduction of eIDAS 2.0, the definitions and requirements for the types of electronic signatures have not changed. Users can still sign electronically using three types of electronic signatures: simple, advanced and qualified electronic signatures.[74] The qualified electronic signature is legally defined as an advanced electronic signature (which meets the requirements of Article 26 eIDAS 2.0) created with a qualified electronic signature creation device and based on a qualified certificate for electronic signatures.[75] An electronic signature creation device is configured software or hardware.[76] The electronic signature creation device is considered qualified if it meets the requirements of Annex II of eIDAS 2.0.[77] A qualified certificate contains a fixed set of (personal) data, including the name of the signatory or a pseudonym and data for the validation of electronic signatures. CBS meet these requirements because they use a (qualified) certificate and are therefore equivalent to a 'wet' signature.[78] The requirement for a qualified certificate means that a user can at least apply a CBS with their wallet.

It is possible to provide an electronic signature, after which the user can simultaneously or immediately after signing also show an attribute to authenticate themselves.[79] The user then shares both the certificate for the qualified electronic signature and the personal data contained therein, as well as the attribute. However, the attribute is not linked to the document, as is the case with ABS. eIDAS 2.0 thus requires a system that allows for the accumulation of additional personal data, but not a reduction in personal data.[80] This is not in line with the principle of data minimisation.[81]

Finally, eIDAS 2.0 explicitly states that the use of pseudonyms is not prohibited in principle.[82] Pursuant to Article 3(14) of eIDAS 2.0, it is therefore possible to sign with CBS using a pseudonym, so that the user is not directly identifiable.

3. The possibilities of ABA and ABS under eIDAS 2.0

The previous section explained what changes eIDAS 2.0 has brought about for trust services via electronic authentication and signing. In this section, I analyse whether the possibilities of ABA and ABS can be exploited under eIDAS 2.0 or whether there are still limitations. This includes decentralised storage, modular identity, signing with a pseudonym or non-identifying attribute, and unlinkability. I will look at both eIDAS 2.0 and the accompanying European Implementing Acts.[83] These Implementing Acts must be regularly evaluated and updated considering new technologies, practices or standards.[84]

3.1 Modular identity

[73] ibid, recitals 19, 20 and art 5a(5)(g).

[74] ibid, arts 3(10), 3(11), 3(12).

[75] ibid, art 3(12), 3(15).

[76] ibid, art 3(22).

[77] ibid, art 3(23).

[78] ibid, art 3(15) and Annex I.

[79] ibid, recitals 19, 74.

[80] The qualified certificate contains, among other things, information about the qualified trust service (eIDAS 2.0, Annex I(b)), the name or pseudonym of the user (Annex I(c)) and data for the validation of the electronic signature (Annex I(d)).

[81] eIDAS 2.0 (n6), recitals 9, 12 and GDPR, art 5(1)(c).

[82] ibid, recital 60 and art 5.

[83] On 21 November 2024, the first implementing acts at European level were adopted. The second set of implementing acts were published on 28 November 2024, the third set on 6 May 2025, the fourth set on 29 July 2025, the fifth set on 29 September 2025 and the sixth set on 27 October 2025.

[84] eIDAS 2.0 (n6), recital 75.

One of the characteristics of ABA and ABS is that they use separate attributes instead of a fixed set of (personal) data from the user, as in a certificate. With the introduction of the European wallet in eIDAS 2.0, a modular identity based on ABA has been realised.[85] Users can authenticate themselves for access to online services using the individual attributes in their wallets.[86] These can be both identifying and non-identifying attributes. European wallets must enable users to selectively disclose attributes.[87] To this end, the standards in Annex II must be implemented in such a way that the wallets support this function.[88] The wallets thus make it possible to create a modular identity. This gives the user control over which attributes they want to share with relying parties, without having to immediately reveal their full identity.[89]

The European wallet also provides users with access to an application for creating a qualified electronic signature.[90] The applications for creating signatures can be integrated directly into the wallet provider[91], be a separate app on the user's device, or be provided remotely.[92] However, eIDAS 2.0 does not allow users to apply ABS that qualify as a qualified electronic signature.[93] This is because eIDAS 2.0 also requires a certificate for applying a qualified electronic signature.[94]

In principle, ABS can qualify as advanced electronic signatures because they can meet the requirements in Article 26 of eIDAS 2.0. However, ABS do not use certificates for validation, but qualified attestations of attributes. Under eIDAS 2.0, ABS therefore cannot be equated with a wet signature.

ABS cannot legally meet the requirement for a qualified certificate (like CBS) because ABS do not use a certificate for validation, but rather a qualified attestation of attributes.[95] This is unfortunate, given the advantages and functions of ABS. Moreover, this restriction is unnecessary, as the intended goal is technically feasible. The requirements for qualified attestations of attributes are strict[96] and practically the same as the requirements for a qualified certificate.[97] It would therefore be possible to consider qualified attestations as qualified certificates. In that case, it is necessary for European wallets to make it legally possible to sign with them. Unfortunately, nothing about this is included in eIDAS 2.0.[98]

Article 28(3) of eIDAS 2.0 explicitly states that it is possible to add optional additional specific attributes to qualified certificates for electronic signatures. However, the restrictions that limit the information that relying parties may request must be taken into account.[99] eIDAS 2.0 offers the possibility of storing certificates in European wallets but does not make this mandatory.

This makes it possible for a user to sign with a CBS and simultaneously or immediately afterwards show an attribute to the relying party. The attribute is then only valid for a certain period.[100] However, this method does not guarantee non-repudiation, because the validity of the attribute cannot be proven to third parties. The attribute is only showed to the relying party and not registered. In addition, the requirement for a

[85] Authentication with a pseudonym and a non-identifying attribute is also possible.

[86] eIDAS 2.0 (n6), art 5a(4)(a).

[87] Implementing Regulation 2024/2979 (n48), recital 10.

[88] This concerns ISO/IEC 18013-5:2021 and the "Verifiable Credentials Data Model 1.1" from the W3C recommendation of 3 March 2022.

[89] eIDAS 2.0 (n6), art 5a(14).

[90] Implementing Regulation 2024/2979 (n48), recital 12, art 2(5) defines a wallet user as a user who has control over the wallet unit. Essentially, this is nothing more than a user within the meaning of eIDAS 2.0.

[91] ibid, art 2(10) defines a wallet entity as an application installed and configured on the device or in the environment of the wallet user. The Dutch ID Wallet and Yivi are examples of this.

[92] ibid, recital 12 and art 12(3).

[93] eIDAS 2.0 (n6), art 5a(4)(e).

[94] eIDAS 2.0 (n6), art 3(12); Implementing Regulation (EU) 2024/2979 (n48), recital 12. See also Section 2.3.

[95] Although ABS can satisfy the requirements for an advanced electronic signature under Article 26 eIDAS 2.0, they still cannot be treated as equivalent to a wet signature.

[96] eIDAS 2.0 (n6), art 3(45); Section 2.3.

[97] ibid, arts 3(15), 28, recital 74 refers to an obligation of result in both cases.

[98] eIDAS 2.0 (n6), art 5a(5)(g) only stipulates that a user can create a qualified electronic signature with the European wallet, but does not specify whether this can also be done with the attributes in the wallet.

[99] ibid, arts 5b(2)(c), 5b(3). See also Section 2.1.1.

[100] As long as the session is valid, this attribute cannot be reused by third parties.

certificate means that a user who wants to sign and not just show an attribute (see section 3.3 for more on this difference), must always share all the data in the certificate. eIDAS 2.0 does not facilitate modular identity for electronic signatures in this way.

3.2 Pseudonyms

ABA with a pseudonym is possible under eIDAS 2.0. If user identification is not required, relying parties may not refuse the use of pseudonyms for authentication.[101] At the request of a relying party, wallet entities do support the generation of a pseudonym that is specific and unique to that relying party.[102] The authentication of specific pseudonyms allows the user to avoid providing unnecessary information to relying parties.[103]

In addition, eIDAS 2.0 makes it possible to sign with pseudonyms in a certificate, but does not require this.[104] Since eIDAS 2.0 explicitly states that the electronic signature must be linked to a specific individual (which can be either an identified person or a pseudonym), European wallets must include a function to generate pseudonyms chosen and managed by the user in accordance with the technical specifications of Annex V of Implementing Regulation 2024/ 2979.[105]

3.3 Non-identifying attribute

For access to online services, it is possible to show only non-identifying attributes (Section 3.1). However, showing attributes alone does not offer the same guarantees as qualified electronic signatures. Showing attributes only guarantees the authentication of the user: the user can prove that he possesses a certain attribute. In some cases, though, it may be necessary to also guarantee the integrity of a message and its non-repudiation without revealing the user's identity. If a user wants to use a social media platform, they must prove that they are of the required age. When the social media platform (the relying party) must subsequently prove that the user was indeed of the required age (integrity) and that the user cannot deny this (non-repudiation), age verification with an ABS can offer a solution.[106] Another example concerns the situation in which a medical professional signs a request for the removal of a child from their home. By signing with an ABS, the professional can prove their legal authority (medical professional) (as well as integrity and non-repudiation) without revealing their full identity. This reduces the risk of possible retaliation in such sensitive situations.

Although it is technically possible to apply an ABS with a non-identifying attribute, eIDAS 2.0 still requires a certificate for placing a qualified electronic signature. This means that the information contained in the certificate is always shared (Section 3.1). This can only be the actual identity or a pseudonym (Section 3.2). It is therefore not possible to apply a qualified electronic signature with a selection of attributes, let alone with a non-identifying attribute.[107]

3.4 Decentralisation

One advantage of attributes is that they can be stored decentralised by the user themselves. This allows users to authenticate themselves online and offline and retain control over with whom and when they want to share their attributes. eIDAS 2.0 does not require decentralisation, as the data can be stored locally or in the cloud.[108] The legal text suggests that attributes are stored in the wallet on the user's mobile device.[109] In order to store the attributes securely and decentralised in the wallet instance, the wallet instance must use at least one secure cryptographic means for wallets.[110] It must use this for the management of “critical

[101] Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties, OJ L 7.5.2025, recital 9.

[102] Implementing Regulation (EU) 2024/2979 (n48), art 14(2).

[103] ibid, art 14. See also Baum (n3) 94.

[104] eIDAS 2.0 (n6), art 3(14). See also eIDAS 2.0, recitals 19, 60 and art 5a(4)(b).

[105] Implementing Regulation (EU) 2024/2979 (n48), art 14(1).

[106] Yong Yong Hu, ‘Juridische eisen aan de betrouwbaarheid van digitale toestemming in de AVG’ (2022) Computerrecht 86-96; See also Section 2.2.2.

[107] Implementing Regulation (EU) 2024/2979 (n48), recital 12; Section 2.3.

[108] eIDAS 2.0 (n6), recital 30.

[109] ibid, recital 19 and arts 5a(4)(a), 5a(4)(b). See also Okamoto and Takashima (n 24) 126-127.

[110] Implementing Regulation (EU) 2024/2979 (n48), art 4(1).

assets" such as the private keys used to create an electronic signature.[111] Essentially, this is nothing more than a tamper-proof device that provides an environment for a secure cryptographic application, such as a mobile phone.[112] Secure cryptographic applications are important for the protection of critical assets and the display of electronic attestations of attributes.[113]

Wallet providers must also ensure that secure cryptographic applications for wallets can, among other things, securely generate new cryptographic keys (subsection c) and generate proof of possession of private keys (subsection e).[114] When wallet providers decide to provide a secure cryptographic application to an embedded secure element, they shall base their technical solution on the technical specifications in Annex I or other equivalent technical specifications.[115] In addition, the wallet provider must ensure that each wallet unit[116] contains wallet unit attestations with public keys and that the corresponding private keys are protected by a secure cryptographic means for wallets.[117]

Logging is not decentralised, as users only have access to a log of all transactions carried out with the European wallet via a common dashboard.[118] The wallet authority must also record all transactions with relying parties, including electronic signatures.[119] The recorded information consists of at least: the date and time of the transaction (subsection a), the names of the contact person and unique identification code of the relying party (subsection b), the type of data requested in the transaction (subsection c) and, if applicable, the reason for non-completion (subsection d).[120] Wallet providers must guarantee the integrity, authenticity and confidentiality of the recorded information.[121] The provider is therefore aware of the usage of all users and is a vulnerable privacy hotspot. This undermines the advantages of decentralised storage.

3.5 Unlinkability

A significant advantage of ABA and ABS is the ability to use unique key pairs to ensure the unlinkability between the user and the attribute or electronic signature.[122] Even though multi-show unlinkability and user unlinkability contribute to user privacy, these forms of unlinkability have not yet been realised and are not required under eIDAS 2.0 and the toolbox with a technical Architecture and Reference Framework (ARF framework).[123] This ARF framework includes a set of common standards, technical specifications, guidelines and best practices that serve as the basis for eIDAS 2.0.[124] The ARF framework is not binding on Member States and serves only as a reference for creating common conditions for the implementation of European wallets.[125] The ARF framework is a living instrument, which means that it remains unclear whether the above forms of decoupling will be included in the ARF framework at a later stage.

[111] ibid, art 2(3).

[112] ibid, art. 2(12).

[113] ibid, recital 6.

[114] ibid, art 5(1).

[115] ibid, art 5(2).

[116] A wallet unit is a term that appears in the Implementing Acts, but is essentially nothing more than the European wallet as an application on a mobile device.

[117] Implementing Regulation (EU) 2024/2979 (n48), arts 6(1), 6(2).

[118] eIDAS 2.0 (n6), art 5a(4)(d). See also Implementing Regulation (EU) 2024/2979 (n48), recital 11.

[119] Implementing Regulation (EU) 2024/2979 (n48), art 9(1).

[120] ibid, art 9(2).

[121] ibid, art 9(3).

[122] See also Gergely Alpár and Bart PF Jacobs, 'Credential Design in Attribute-Based Identity Management' in Ronald Leenes (ed), *Bridging Distances in Technology and Regulation* (Wolf Legal Publishers 2013) 189–204.

[123] eIDAS 2.0 (n6), recital 14 only states that ZKP technology can offer a solution, without specifying how this can be incorporated. See also Baum (n39).

[124] European Commission, 'European Digital Identity Wallet: Architecture and Reference Framework' (Version 2.4.0, 2024) https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/architecture-and-reference-framework-main/#24-qualified-electronic-signatures accessed 25 July 2025.

[125] ibid, see section 1.2.

4. Conclusion

More and more activities are taking place online. A reliable authentication process is therefore of great importance. The old legal framework of eIDAS 1.0 did not facilitate attribute-based authentication and signing and its various advantages. The European Commission recognised that eIDAS 1.0 needed revision and therefore introduced eIDAS 2.0 in May 2024. This article highlights the characteristics of attribute-based authentication and signatures and examines the extent to which these characteristics are also facilitated in the context of eIDAS 2.0. I answer the following research question: 'To what extent does eIDAS 2.0 facilitate the utilization of the possibilities and advantages of attribute-based signatures?

eIDAS 2.0 creates a few preconditions for the use of ABA and ABS. For example, eIDAS 2.0 offers the possibility of using attributes in European wallets for access to online services and digital signing (Section 2.3). Enabling these two functions in a single European wallet increases ease of use for users. The use of ABA is fully realised under eIDAS 2.0, as users can show individual attributes to relying parties to authenticate themselves. Users can have a modular identity and share specific personal data with relying parties (Section 3.1). In addition, attributes can be stored decentralised on the user's mobile device, thereby guaranteeing autonomy (Section 3.4).

Unfortunately, not all the advantages of using ABS are realised under eIDAS 2.0. eIDAS 2.0 and the implementing acts do not equate signing using ABS with qualified electronic signatures. As a result, users are dependent on CBS, which always involves a certificate with a fixed set of personal data. This undermines the principle of data minimisation (Section 3.1). In addition, the possibility of signing from different roles remains unexploited, which is a missed opportunity (Section 2.2.2). It is also not possible to sign with a non-identifying attribute (Section 3.3). Furthermore, eIDAS 2.0 does not require decentralisation, which means that logging is not regulated in a decentralised manner (Section 3.4). Finally, eIDAS 2.0 currently cannot guarantee multi-show and user unlinkability, which does not benefit user privacy (Section 3.5).

There is room for improvement when it comes to facilitating ABS in eIDAS 2.0. To this end, the European Commission must first take a critical look at the definition of a qualified electronic signature. The current emphasis on certificates excludes the use of separate attributes as a qualified electronic signature. This is unnecessary, as the requirements for qualified attestations of attributes are just as strict as the requirements for qualified certificates. In addition, allowing the use of non-identifying attributes in electronic signatures would significantly increase user privacy. By using ABS, the linking of the user and the electronic signature can be prevented, and users gain maximum control over what information they want to share with relying parties. Given that all Member States must have at least one European wallet by 21 November 2026 at the latest.[126] It is important that further details are provided on the regulations and implementing acts that actively support ABS. Without further development, we will have to wait for eIDAS 3.0 before a truly future-proof, user-friendly and privacy-friendly framework for digital identity, including signing, can be established within the EU.

[126] eIDAS 2.0 (n6), art 5a(1).