Dutch Payments Association

The EU Digital Identity Wallet in payments: Interpretation of legislators' intention and feasibility assessment

Industry view (not a legal position)

eIDAS 2.0 Taskforce
Dutch Payments Association

Amsterdam
21-05-2025

Content

Dutch Payments Association

This paper highlights the gap between intended scope and feasibility of acceptance of the EUDIW in payments, and asks for more clarity

Dutch Payments Association

A dedicated eIDAS 2.0 taskforce was set up by the Dutch Payments Association

The Dutch Payments Association established a taskforce (TFeIDAS) with several members to assess the impact of the European Digital Identity Wallet (EUDIW) on payment processes. The goal is to provide industry guidance by interpreting the intended scope of acceptance of the EUDIW in payments, required by eIDAS 2.0. This paper does not provide a legal interpretation of our position on the scope of acceptance and should not be viewed as one.

While the text of the eIDAS 2.0 regulation and the first set of implementing acts regarding the EUDIW are finalised, a conclusive interpretation of the scope of acceptance and impact on payments remains unclear. The challenge for Payment Service Providers (PSPs) lies in navigating this ambiguity and preparing for the impact and implementation of the EUDIW. In light of this, members of the association have come together in this taskforce to develop a view on the intended scope of acceptance of the EUDIW on payments to get a first view on the possible compliance requirements for banks. The taskforce regarded the intended scope of acceptance of the EUDIW for PSPs in the context of their payment processes in two dimensions: 1. Interpretation of the legislator's intended scope w.r.t. payments. 2. The feasibility for PSPs to comply with eIDAS 2.0, while also complying with the requirements laid down in PSD2 and the RTS on SCA.

This first industry view is based on the TF interpretation of the given context and the legislative text. Its primary objective is to share knowledge and provide guidance to our members and other PSPs on how to understand the intended scope of acceptance of the EUDIW in relation to payments. During the development of this paper, the taskforce identified a gap between the intended scope of acceptance and the practical challenges of meeting the SCA requirements laid down in PSD2 and the dedicated RTS on SCA. Therefore, another key objective of this paper is to highlight this gap and request further clarity and guidance from EU co-legislators. Finally, the paper aims to make a clear distinction between elements that are part of compliance efforts with eIDAS 2.0 and elements that are beyond compliance and thus optional for PSPs.

Sources: eIDAS revision

The scope of this paper is limited to payment processes for natural persons as holders of EUDIWs. The paper does not address compliance topics related to legal entities as holders of EUDIWs. The paper also does not address topics such as managing fraud, liability, security and other implementation challenges. Furthermore, while KYC for onboarding is recognised as part of the interpreted intended acceptance scope, the taskforce has not conducted a thorough analysis on this topic, as our focus has primarily been on payments. Therefore, additional analysis would be needed to assess the exact impact and implementation of the EUDIW in the onboarding context.

This paper includes terms that can have different interpretations depending on the context, such as online identification, authentication, authorisation, and payment initiation. To minimise the risk of misunderstanding our paper, Appendix I contains a list of definitions that we use specifically in the context of this implementation guidance paper.

Throughout the paper, we refer to 'PSPs' as being relying parties (RPs) in scope of eIDAS 2.0 in a payment context. More specifically however, the impact of acceptance is on account servicing payment service providers (ASPSPs), these are mostly banks.

This paper was co-created by the following parties as members of the TFeIDAS:

ABN·AMRO | de volksbank
ING | Rabobank
Dutch Payments Association | INNOPAY A business of Oliver Wyman

Summary – Intended acceptance of EUDIW in payments while adhering to PSD2 SCA requirements appears impossible

Dutch Payments Association

On April 30, 2024, the approved revision of the eIDAS regulation, referred to as 'eIDAS 2.0', was published in the Official Journal of the EU. The revision introduces the EUDIW, which must be available for issuing by all EU Member States to both natural and legal persons who wish to obtain and use one. EUDIWs are intended to serve as an identification and authentication tool for accessing online public and private services across the EU.

The regulation requires a designated list of private service providers, among those in the banking and financial services sector, to accept and integrate EUDIWs. This applies to those processes where strong user authentication (SUA) for online identification is required by contract or law and comes with a deadline of December 24, 2027. This deadline was formalised on the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) (20 days after publication on December 4, 2024).

Intention of the legislator

The legislator intended that PSPs must integrate EUDIWs in processes where strong customer authentication (SCA) is required by e.g. revised Payment Services Directive (PSD2) or Anti-Money Laundering Directive (AMLD) for online identification.

Complication

The integration of the EUDIW into processes requiring SCA can be complex, especially because use of the EUDIW must always be offered as an additional option next to the existing processes and PSPs have to comply with additional SCA requirements as laid down in PSD2. Still, the added value of the EUDIW as additional means of SCA remains unclear in many payment flows. Considering this complexity and the lack of clarity on how EUDIWs should be integrated, PSPs are concerned about operational adjustments needed to comply with the new regulation. The taskforce established that it is a pre-condition that clarity is provided on these topics. A successful and workable implementation and roll-out of the EUDIW as an authentication and identification method for payment services is not possible without guidance and clarity on how to comply with both eIDAS and the RTS on SCA and how to deal with topics such as fraud and liability.

TFeIDAS reached several conclusions

Based on eIDAS art. 5f(2), a legal comparison of Strong User Authentication (SUA, eIDAS2) and Strong Customer Authentication (SCA, PSD2) and the TF's definition of online identification, the taskforce reached the following conclusions regarding the interpreted intended scope of the legislator:

1. SUA refers to the concept of two-factor authentication (2FA), but 2FA is only a small part of the complex concept that is SCA for payment services
2. The EUDIW is intended to be accepted as a 2FA tool in processes where SCA for online identification is required
3. PSD2 art. 97(1) requires PSPs to apply SCA in multiple steps of online (payment) processes. Thus, the EUDIW is intended to be accepted as 2FA tools for these (payment) processes when it falls in scope of online identification:
    1. SCA to access a payment account online
    2. SCA to initiate electronic payment transactions
    3. SCA to carry out remote actions which may imply a risk of fraud

The taskforce reached further conclusions regarding the implications and feasibility of the interpreted intended scope:

1. The intended acceptance of the EUDIW mandated by eIDAS 2.0, namely as 2FA tool, while adhering to the SCA requirements laid down in PSD2/RTS on SCA appears impossible for PSPs at this moment. More clarity and guidance is required to determine how to utilise the EUDIW within the payment context while complying with PSD2 RTS requirements
2. Besides accepting the EUDIW as a 2FA tool in processes where SCA for online identification is required, eIDAS 2.0 does not impose any additional acceptance obligations of other wallet functionalities on PSPs, such as acceptance of electronic attestations of attributes (EAAs) or electronic signatures. There is also no requirement for PSPs to issue EAAs
3. The taskforce recognises future innovation potential for the EUDIW in the context of payments, but this is beyond the compliance responsibilities for PSPs

According to eIDAS 2.0, EUDIWs must be accepted wherever 2-factor authentication is applied for online identification

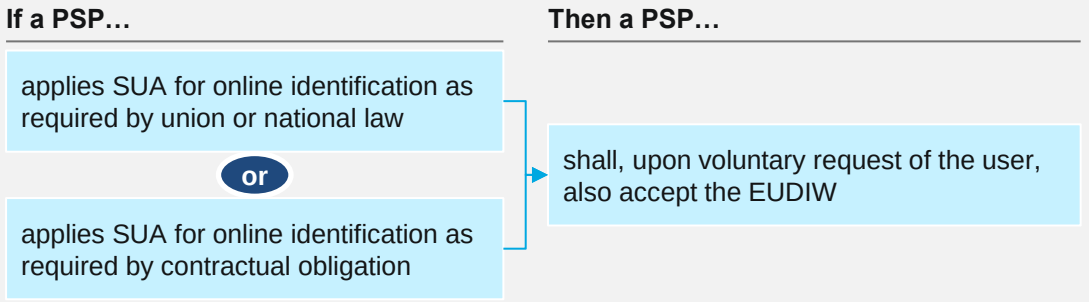
Dutch Payments Association

Introduction eIDAS 2.0 - How is it relevant for payments?

On 30 April 2024, the European Digital Identity Regulation – often referred to as eIDAS 2.0 – was published in the Official Journal of the EU as a revision to the eIDAS regulation. The most notable aspect of this revision is the introduction of the EUDIW, which must be mandatorily issued[1] by all EU Member States and offered to both natural and legal persons[2] on a voluntary basis. EUDIWs should serve as an additional means of identification and authentication towards both public and private services within the European Union.

eIDAS 2.0 introduces a requirement for relying parties to accept the EUDIW for processes that currently involve SUA, described in article 5f(2). The part of art. 5f(2) relevant for PSPs states the following: *"Where private relying parties that provide services […] are required by Union or national law to use strong user authentication for online identification or where […] required by contractual obligation, including in the areas of […] , banking, financial services, […] , those* ***private relying parties shall*** *[…]* ***also accept European Digital Identity Wallets*** *[…]"*

Figure 1: *When should a PSP accept the EUDIW?*



eIDAS mandates PSPs to accept the EUDIW as of 24 december 2027

Relying parties, including PSPs, are expected to accept the EUDIW next to existing solutions where SUA for online identification occurs as of 24 December 2027. What this means for PSPs is still unclear. The regulatory Technical Standard (RTS) to be developed by the European Banking Authority (mandated under the Payment Services Regulation (PSR)) could provide additional clarity, but will likely only be applicable after this date.

SUA refers to the concept of 2FA

Following the legal definition of SUA in eIDAS2.0 (as outlined on the next slide), SUA directly refers to the concept of two-factor authentication (2FA). This is a security process in which a user is required to provide two distinct forms of identification to verify their identity when accessing an account or system, combining factors from different categories of either knowledge (something only the user knows), possession (something only the user possesses) or inherence (something the user is). Article 5f(2) of eIDAS2.0 can be interpreted as an obligation to accept the EUDIW where relying parties are required to apply 2FA, either by law or by contract.

To clarify the acceptance of the EUDIW in the context of payments, we must address two fundamental questions:

1. How does the concept of SUA relate to the context of payments? In other words, in what parts of payments processes are PSPs required to apply 2FA?
2. What is the scope of online identification?

We address these questions in slide 6-8. After addressing these questions and interpreting the legislators' intentions, we assess the feasibility of the interpreted intended scope of acceptance in slide 9.

Sources: eIDAS revision

[1] = Each Member State shall issue an EUDIW in one or more of the following ways: (1) government-operated, (2) outsourced or (3) recognition of market solutions | [2] = The paper does not address compliance topics related to legal persons as holders of EUDIWs

SUA refers to the concept of 2FA, whereas 2FA is only a small part of the complex concept that is SCA for payment services

Dutch Payments Association

SCA occurs in multiple steps of online (payment) processes

In the context of payments, PSD2 introduces SCA which builds upon the concept of 2FA and includes additional requirements for PSPs. 2FA is an important part of the full scope of SCA. Figure 2 aims to highlight the difference between 2FA in the context of SUA and SCA. Following the reasoning in eIDAS art. 5f(2), the EUDIW should be used as a 2FA tool in payment processes where (i) SCA is mandated by PSD2 and (ii) the specific authentication is considered as 'online identification' (page 8). The taskforce interprets the intention of the eIDAS2.0 legislator that the EUDIW must be accepted as a 2FA tool in online (payment) processes where SCA is required (as defined in article 97 paragraph 1 of PSD2) for online identification. We refer to '2FA tool' as the EUDIW could serve as a tool for performing the two-factor authentication part of what is the complete set of requirements that is SCA under PSD2/RTS.

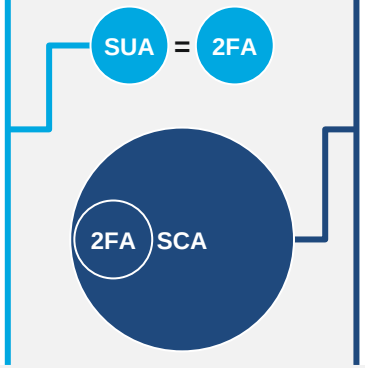
This means the EUDIW is intended to be accepted as a 2FA tool in the following processes (when regarded online identification), defined in art. 97(1) PSD2:

1. **SCA to access a payment account online:** When an existing customer wants to 'login' to their banking environment, SCA is applicable (EUDIW use is subject to prior binding of the wallet for this purpose)
2. **SCA to initiate electronic payment transactions:** When a customer wants to initiate a payment and authenticates and authorises the transaction
3. **SCA to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses:** When a customer wants to perform non-payment actions such as changing a pin code or increasing spending limit

The payment flow on the next slide shows a visual example of the interpreted intended scope of the EUDIW, which we currently deem unfeasible.

Figure 2: *Difference between 2FA in the context of SUA or SCA*

'strong user authentication' means an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;



'**strong customer authentication**' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

Requirements to be **complied with by payment service providers** for the purpose of implementing security measures which enable them to apply the procedure of strong customer authentication in accordance with Article 97 of Directive (EU) 2015/2366 (PSD2)

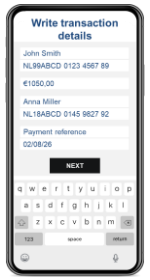
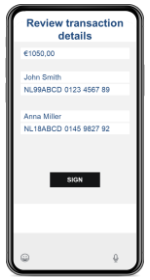
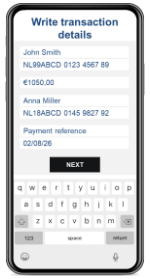
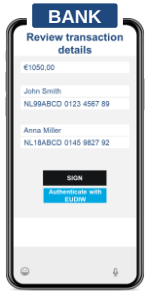
Where **payment service providers apply strong customer authentication in accordance with Article 97(2)** of PSD2, in addition to the requirements of Article 4 of Delegated Regulation (EU) (2018/389) (further referred to as 'RTS on SCA'), they shall also adopt security measures that meet additional requirements

Sources: eIDAS revision, PSD2, AMLD5, PSD2 RTS SCA

The EUDIW is intended to be accepted at multiple points in payment flows, even if it does not enhance user experience

Dutch Payments Association

Interpretation of intended flow, currently not feasible

	1. Access a payment account online	2. Write details of the transaction	3. Review transaction details	4. Initiate a payment
Existing flow				
Or				
Intended EUDIW flow				*Note that authentication (via the EUDIW) and authorisation of the payment transaction (in the bank environment) are separated in the intended EUDIW flow. More guidance is needed to comply with PSD2 RTS while using the EUDIW.*

Interpreted intended scope

The legislator intends for the EUDIW to be used as a 2FA tool in payment processes where SCA for online identification is mandated by PSD2. In the above hypothetical example, this takes place at two points: (1) when accessing a payment account online, and (2) when authenticating to authorise a payment transaction. In the context of the Netherlands, this intended scope does not enhance the user experience for customers; instead, it diminishes it by requiring more redirects and making the process less seamless.

Sources: eIDAS revision, PSD2

The EUDIW should only be accepted in payment transactions with an online network connection and user experience

Dutch Payments Association

What is the scope of online identification?

Understanding what 'online identification' entails is the next step in classifying where the EUDIW is intended to be accepted. The eIDAS 2.0 legal text and associated documentation do not provide a definition for 'online identification'. In the realm of digital identity, we traditionally distinguish between identification (claiming your identity), authentication (verifying your identity), and authorisation (determining access to actions or resources). We interpret the 'identification' aspect of 'online identification' as referenced in eIDAS to encompass both identification and authentication, but not authorisation.

eIDAS 2.0 does however define 'electronic identification', which provides guidance. It is defined 'as the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person'. Furthermore, in the eIDAS2.0 legal text authentication is defined as a confirmation of electronic identification. We therefore conclude that electronic identification can either be 'online identification' or 'not-online identification'.

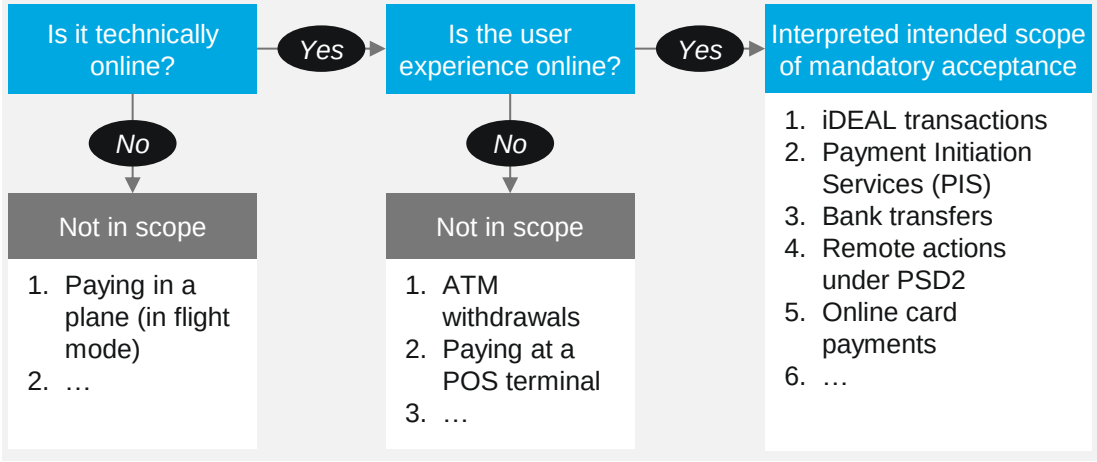
Two perspectives are available when defining online versus not-online identification

In assessing whether we speak of 'online identification' or 'not-online identification' in a payments context, the taskforce considered two perspectives:

1. **Technical perspective**: Whether identification is 'online' depends on how the identification is technically performed.
   - Online: if currently, the process of identification as required by law or by contractual obligation can only be completed successfully using an 'online' real-time network connection, enabling exchange of data between the point of interaction and back-end systems essential to the identification process, then we deem this 'online identification'
   - Not-online: identification is completed locally, without the use of an online network connection; for example: based on the EMV chip or based on two-factor through a personalised app
2. **User experience perspective**: Whether identification is 'online' depends on the interaction between payer and payee during the identification process, i.e. whether the actual identification takes place in an online channel/environment or physically.
   - Online: user is not in the physical presence of his transaction counterpart
   - Not-online: user is physically present in the same place as his transaction counterpart (i.e. at the point of interaction)

Figure 3 shows part of the interpreted intended scope of acceptance of the EUDIW.

Figure 3: *Defining online identification to determine interpreted intended scope*



Conclusions on scope of online identification

Based on both the technical as well as the user experience perspective, the taskforce concluded that only transactions that are online from both perspectives (technical and user experience), are in scope of 'online identification'. Hence, the EUDIW is intended to be accepted as a 2FA tool for SCA in transactions with an online network connection and online user experience. Acceptance of the EUDIW is not intended for any 'offline' situation.

Since implementing the interpreted intended scope is currently not feasible, additional guidance from the regulator is required

Dutch Payments Association

Feasibility of the interpreted intended scope

While the legislator's intention of the acceptance scope is quite clear – the EUDIW is intended to be accepted as a 2FA tool in processes where SCA for online identification is required – it is considered impossible to comply with the legal requirements of eIDAS 2.0, given the current legal requirements from PSD2 and the Regulatory Technical Standard (RTS) on SCA. The inability to comply with both eIDAS 2.0 and PSD2 is mainly because the RTS on SCA does not cater for dedicated 2FA tools as part of a larger flow for SCA. This means certain requirements of the RTS on SCA cannot be fulfilled by an EUDIW.

Request for clarity and guidance from EU co-legislators

Based on this identified gap, further clarification from DG FISMA and/or the EBA is needed on how to proceed. First, guidance is needed on how requirements on control can be applied or will be waived when using the EUDIW. Second, clear guidance on how to embed the EUDIW as a 2FA tool for SCA for online identification when initiating an electronic payment transaction (PSD2 art. 97(1)(b)) and other risky remote actions (PSD2 art. 97(1)(c)), in such a way that meets the requirements of the RTS on SCA.

Table 1 highlights the difference between the (i) interpreted intended scope of acceptance and (ii) the legally possible scope of acceptance for each of the processes, considering the legal requirements from PSD2 and the RTS on SCA.

Feasibility EUDIW as means for SCA of the interpreted intended scope

Several market actors argue that the EUDIW could serve as fully SCA-compliant means. We tend to disagree on this. The EUDIW can serve as a means to perform 2FA, while SCA goes beyond 2FA. Banks are not able to fulfil several other requirements of the RTS on SCA:

1. **Banks do not have the ability to control EUDIWs**: The RTS on SCA contains requirements that state that the PSP must ensure the safety, security, confidentiality of personalised security credentials. PSPs are unable to ensure this when the EUDIW falls outside of their domain
2. **EUDIWs lack certain functionality**: The RTS on SCA contains requirements such as dynamic linking that cannot be fulfilled by EUDIWs because they lack the functionality to meet these requirements

Table 1: *Difference between interpreted intended scope of acceptance and the possibility to comply with eIDAS and PSD2*

Interpretation of intended scope of acceptance of the EUDIW as a 2FA tool for (when it considers online identification):		Example flows	Possible to comply with both legal requirements
1	**SCA to access a payment account online**	Logging into a bank account	1 2
2	**SCA to initiate electronic payment transactions**	Bank transfers, online transactions, eMandates	1 2
3	**SCA to carry out remote actions which may imply a risk of fraud**	Changing your spending limit	1 2

1 = Possible to comply with PSD2 as banks do not need to have control over the personalised security credential

1 = Not possible to comply with PSD2 as banks must have control over the EUDIW as personalised security credential*

2 = Possible to comply with PSD2 as the EUDIW supports the required functionality/data

2 = Not possible to comply with PSD2 as the EUDIW does not support the required functionality

Sources: eIDAS revision, PSD2, PSD2 RTS SCA, eIDAS implementing Act integrity and core functionalities * According to The RTS on SCA

We must distinguish the facts from fiction when it comes to acceptance of EUDIWs for PSPs

Dutch Payments Association

Since the publication of eIDAS2.0, there has been considerable discussion about payments in relation to the EUDIW. However, with the release of the implementing acts related to EUDIW functionality, it has become clearer what the intended acceptance entails for PSPs and what it does not.

Considerations beyond the scope of eIDAS 2.0, including other regulations such as the PSR or speculation about the functionalities of wallets in general, are not relevant when assessing the acceptance impact of the EUDIW on PSPs. The interpreted intention of the legislator is that PSPs must accept the EUDIW as a 2FA tool for SCA compatible across Europe. Besides accepting the EUDIW as 2FA tool for SCA, eIDAS 2.0 does not impose any additional acceptance obligations of other wallet functionalities, such as accepting EAAs or electronic signatures, for instance for payment authorisation purposes. The actual initiation of a payment transaction with an EUDIW also falls outside the scope of acceptance. While not in scope of acceptance, utilising the EUDIW for acceptance of EAAs could present valuable use cases for PSPs.

Furthermore, if one EUDIW decides to include functionalities and standards beyond the current scope of eIDAS and its implementing acts, it does not make the additional functionalities mandatory for acceptance by relying parties. Take for example the payment use case that is being researched in multiple EU Large Scale Pilots (LSPs). Any payment use case that requires additional standards or specifications to function is out of scope and not part of the mandatory acceptance. All EUDIWs must support only ISO/IEC 18013-5:2021 and the Verifiable Credentials Data Model 1.1. As a result, use cases that require additional standards or specifications (such as EMV or FIDO standards) are always beyond compliance.

In general, we understand the mandate of LSPs to encompass the piloting and testing of the EUDIW across a range of use cases, including payments. Based on these activities, LSPs are expected to provide feedback to the European Commission for the ARF and Reference Implementation. We consider any solutions provided by the LSPs to comply with eIDAS 2.0 to be voluntary for the industry to adopt. A minority of stakeholders participating in LSPs cannot dictate specific implementations for an entire ecosystem. Lastly, there is no requirement for relying parties to issue EAAs. If a payment use case necessitates that PSPs issue EAAs to function, it will also always be considered a beyond-compliance use case and not part of the mandatory acceptance scope for RPs.

It is worth considering that in June 2023 the European Commission published the Payment Services Regulation (PSR), together with PSD3 the successor of PSD2. Art. 89 PSR mandates the European Banking Authority (EBA) to develop regulatory technical standards (RTS) on i.e. authentication, taking into account the EUDIW, 1 year after entry into force of PSR. As political negotiations on PSR likely will not be finalised by Q4 2025, this RTS will be published too late to provide (additional) guidance on the impact of eIDAS 2.0 on payments. From a functional perspective, besides providing guidance on using the wallet, PSR and PSD3 cannot extend the scope of the wallet functionality, beyond those EUDIW functionalities determined in the relevant implementing acts.

Without additional guidance by the EBA, it is not possible to implement the EUDIW and comply with PSD2.

Beyond compliance: EUDIWs can serve as a building block in the context of payments

We envision that utilising the EUDIW as a building block could enhance many future financial products and services, enabling greater innovation and efficiency in the financial sector. We see many market initiatives and pilots currently examining the potential of the EUDIW beyond mere regulatory compliance. While these projects are not part of the regulatory compliance of mandatory acceptance for relying parties, it is important to continue exploring these beyond-compliance opportunities for innovation and understanding their potential impact. By doing so, we can better prepare for a future where the EUDIW plays a more integral role alongside existing solutions in various financial processes and services.

Sources: eIDAS revision, eIDAS implementing Act integrity and core functionalities

Disclaimer

Dutch Payments Association

Disclaimer

The Dutch Payments Association does not accept any liability to any third party. The opinions expressed in this report are valid only for the purpose stated herein and as of the date of this report. This report reflects our interpretation of the legislator's intended scope w.r.t. payments and should not be treated as conclusive (legal) advice, or legal interpretation. No obligation is assumed to revise this report to reflect changes, events, or conditions, which occur subsequent to the date hereof. All decisions in connection with the implementation or use of advice or recommendations contained in this report are the sole responsibility of the reader.

Contact details

Name: Niels Pranger
Website: https://www.betaalvereniging.nl/en/
E-mail: n.pranger@betaalvereniging.nl
Visiting address: Gustav Mahlerplein 33-35, 1082 MS Amsterdam
Phone number: +31 20 305 1900

May 21, 2025

Appendix I: definitions

Dutch Payments Association

Term	Definition	Source
2FA	A security process in which a user is required to provide two distinct forms of identification to verify their identity when accessing an account or system, combining factors from different categories of either knowledge (something only the user knows), possession (something only the user possesses) or inherence (something the user is)	This paper
2FA tool	A specific software or hardware solution that facilitates the implementation of two-factor authentication (2FA)	This paper
Identification	An act of identifying : the state of being identified	Merriam-Webster
Electronic identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person	eIDAS 2.0 (art. 3(1))
Electronic identification means	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service	eIDAS 2.0 (art. 3(2))
Authentication	An electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form	eIDAS 2.0 (art. 3(5))
Payment initiation	The steps necessary to prepare the execution of a payment transaction, including the placement of a payment order and the completion of the authentication process (similar to 'initiation of a payment transaction' in the Payment Services Regulation (PSR))	PSR – proposal EC (art. 3(6))
Dynamic linking	Elements which dynamically link the transaction to a specific amount and a specific payee	(PSD2) RTS on SCA and CSC – art. 5
Strong user authentication	An authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data	eIDAS 2.0 (art. 3 (51))
Strong customer authentication	An authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data	PSD2 (art. 4 (30))
Payment processes	The entire process from electronic identification to the completion of payment initiation	This paper

Sources: eIDAS revision, Merriam-Webster

Appendix II: abbreviations

Abbreviation	Definition
2FA	Two-Factor Authentication
AMLD	Anti-Money Laundering Directive
ASPSP	Account Servicing Payment Service Provider
ATM	Automated Teller Machine
eIDAS	Electronic Identification, Authentication, and Trust Services
EAA	Electronic Attestation of Attributes
EBA	European Banking Authority
EMV	Europay, Mastercard, and Visa
EUDIW	European Digital Identity Wallet
FIDO	Fast Identity Online
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PIS	Payment Initiation Service

Abbreviation	Definition
PSD	Payment Services Directive
PSP	Payment Service Provider
RP	Relying Party
SUA	Strong User Authentication
SCA	Strong Customer Authentication
TFeIDAS	Taskforce eIDAS

Sources: eIDAS revision