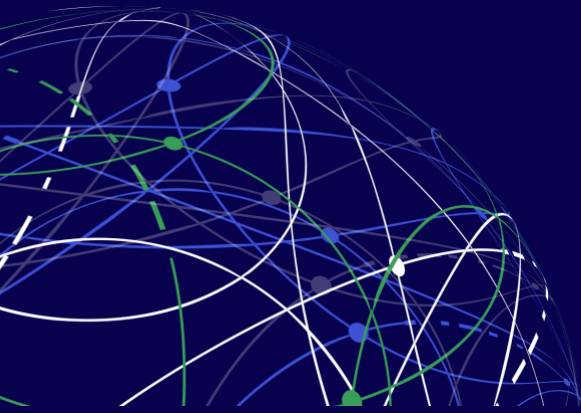


Impact of eIDAS revision and EU Digital Identity landscape on data spaces development

Whitepaper by Centre of Excellence for Data Sharing and Cloud
January 2024



About Authors



Alexander van den Wall Bake
Business Consultant, TNO Netherlands

Alexander van den Wall Bake is a business consultant at TNO and head of the Self-Sovereign Identity portfolio group. He has an extensive background in innovation at large companies. Alexander views innovation from a systemic change perspective where value-driven collaboration is the key to meaningful change.



Vincent Jansen
INNOPAY Netherlands

Vincent Jansen is a managing partner at INNOPAY and has been with INNOPAY since 2003. He is a passionate collaborative innovator and has extensive experience in creating standards, agreement systems and trust frameworks for two-sided products in complex, multi-stakeholder environments.



Leon Kluiters
INNOPAY Netherlands

Leon Kluiters is a consultant at INNOPAY and has experience in the field of digital identity, data sharing and payments. He is part of the Digital Identity Team within INNOPAY, which focuses on wallets, Self-Sovereign Identity and eIDAS regulations.



Yekaterina Travkina
INNOPAY Netherlands

Yekaterina Travkina is a consultant at INNOPAY specialising in research on trust, governance, and digital identity for data spaces. She is supporting CoE-DSC use cases track as part of CoE-DSC harmonisation efforts to foster data spaces development.

About Contributors

The insights that were gained while drafting this whitepaper were validated with the help of experts from various fields. Below you can find the list of all contributors who were part of the interview research process that led to this whitepaper. The authors of this document would like to thank these experts for their contribution and sharing their knowledge.

Experts from data spaces:

- BDI DIL
- Catena X
- DSGO
- HDN
- MFFBAS
- SBR Nexus
- SCSN

Representatives of technology providers:

- iSHARE
- Cleverbase
- Ledger Leopard
- Sphereon

Experts from EU legislative groups:

- DSSC

Table of Contents

Management summary	5
Introduction	6
Reading guide	6
Chapter 1. Context of the eIDAS regulation	8
<i>What does eIDAS regulation and its revision mean for IAA in data spaces?</i>	8
1.1 Digital Identity is an important building block for data spaces	8
1.2 eIDAS and its revision bring opportunities to data spaces to enhance their digital identity procedures	10
1.3 The introduction of EDIWs brings new opportunities to many sectors	14
1.4 Organisations in data spaces might face mandatory acceptance of the EDIW	16
1.5 The introduction of EDIWs introduces new opportunities to data spaces	17
Chapter 2. Market perspective	20
<i>What is the state of the EU DI market landscape and what does it bring for data spaces?</i>	20
2.1 eIDAS trust services support trustworthy data sharing in data spaces	20
2.2 Trust services under eIDAS1 help existing data spaces	21
2.3 Trust services under the eIDAS revision provide new opportunities for data spaces	23
2.4 Usage of Trust Services will be essential when working with wallets to verify both issuers and verifiers	24
2.5 Digital identity services outside of eIDAS are also available for data spaces to leverage	26
Chapter 3. Practical steps for data spaces	29
<i>What are practical steps to implement suitable digital identity solutions in a data space in line with regulatory and market perspectives?</i>	29
3.1 Follow a roadmap to get suitable digital identity solutions in a data space	29
3.2 Practical ways for data spaces to stay informed and join conversations on legislative decision making	33
Chapter 4. Recommendations	35
Appendix	36

Management summary

This report explores the impact of the eIDAS revision (eIDAS2)¹ and the evolving EU Digital Identity landscape on data spaces. It emphasises the critical role of digital identity as a fundamental building block for data spaces, analysing how eIDAS regulations, both current and revised, offer opportunities for enhancing digital identity procedures in data spaces.

The report delves into the market perspective, examining trust services under eIDAS and their significance in trustworthy data sharing within data spaces. It presents practical steps for data spaces to implement suitable digital identity solutions, aligning with regulatory and market perspectives.

Data spaces are recommended to do three things to face the impact of the eIDAS revision head on:

1. **Engage proactively with eIDAS regulation:** leverage eIDAS1 and eIDAS2 functionalities to improve your digital identity processes. For data spaces that face mandatory acceptance of the EDIW (EU Digital Identity Wallets), be aware that implementation timelines are short. The issuance of the EDIW is expected at the beginning of 2026. It is recommended to start preparing now and evaluate if your sector faces mandatory acceptance (see paragraph 28 in the eIDAS revision text as of November 2023)
2. **Follow the roadmap to implement suitable digital identity solutions that ensures interoperability in the long run:** Data spaces should explore opportunities while building upon the foundation of eIDAS as a generic way to support digital identity processes in a future-proof and interoperable manner. Leveraging common EU-wide digital identity means allows for easier growth of a data space in terms of new participants. It also enables cross-sectoral data sharing opportunities. Data spaces can follow the roadmap presented in this whitepaper to identify suitable digital identity solutions and stay up to date with regulatory changes.
3. **Foster collaboration and partnerships:** Encourage collaboration and partnerships in and among data spaces, digital identity providers, and regulatory bodies. This collaborative approach can lead to a better understanding of the practical implications of eIDAS and is the key to attain value in the long run.

These recommendations aim to reinforce the strategic approach of data spaces in adapting to eIDAS regulations and the evolving EU digital identity landscape that emerges from those.

¹ [eIDAS revision November 2023](#)

Introduction

Digital Identity (DI) is a key building block for data spaces. In the EU, there are various DI services and standards already available, and even more are being developed. Part of the EU DI market is already regulated by eIDAS¹, covering both trust services and a pan-EU federation of public DI means and their levels of assurance. eIDAS1 is now under revision. eIDAS2 introduces new trust services and a European Digital Identity Wallet (EDIW) for natural persons. It also introduces an Organisational Digital Identity Wallet (ODIW) for legal entities. These wallets enable natural persons and legal entities to store and share verifiable information about their entity. Both will become available to public and private issuing and relying parties.

Considering these upcoming changes, the Centre of Excellence for Data Sharing and Cloud (CoE DSC) aims to create an understanding of implications of these changes for its stakeholders in data spaces (e.g. data sharing initiatives and service providers). In this paper the CoE DSC presents research on the impact from (a) the eIDAS revision² and (b) the EU Digital Identity (DI) landscape on the development of digital identity in data spaces.

The insights established in this report were validated through interviews with the following parties: BDI DIL, Catena X, Cleverbase, DSGO, DSSC, HDN, iSHARE, Ledger Leopard, MFFBAS, SBR Nexus, SCSN and Sphereon. The authors would like to express their gratitude to them.

Reading guide

This report is structured as follows:

- **Chapter 1. Context of the eIDAS regulation** - Covers the importance of digital identity in data spaces as an essential building block, and thereunder shows how eIDAS1 and eIDAS2 affect digital identity in data spaces, as well as introduce new opportunities arising from the introduction of the EU Digital Identity Wallet (EDIW).
- **Chapter 2. Market perspective** – Covers the impact and possibilities that eIDAS Trust Services bring to digital identity of data spaces and presents various practical use cases for eIDAS1 and eIDAS2 trust services, as well as other services available in the market.
- **Chapter 3. Practical steps for data spaces** – Covers a roadmap that data spaces can follow to establish suitable digital identity implementations in their data space and stay informed about regulatory changes and new developments.
- **Chapter 4. Conclusions & recommendations** – Provides recommendations and summarises overall awareness and readiness of data space participants and technology providers regarding changes from the eIDAS revision.

² [European Commission](#)

Limitations of the research and next steps




The whitepaper's recommendations emphasize the importance of aligning data spaces with eIDAS. It is essential that data spaces not only meet compliance requirements but also leverage the possibilities offered by eIDAS. This approach will improve digital identity management and security within their data space. It also paves the way for interoperability across various sectors in the future.

In that regard, further research work is needed to assess (and potentially align) the eIDAS identity management developments with the developments in the EU Data Strategy initiatives like Data Space Protocol, IDSA, Gaia-X, DSBA, DSSC-Blueprint, SIMPL.

Chapter 1. Context of the eIDAS regulation

What does eIDAS regulation and its revision mean for IAA in data spaces?

This chapter will present eIDAS1 and eIDAS2 to depict its relevance for the digital identity in data spaces. In accordance with the DSSC (Data Spaces Support Centre), hereunder, digital identity is presented as one of the building blocks for the data spaces' development, facilitating the processes of Identification, Authentication and Authorisation (IAA).

Chapter 1 focus areas:	What does it mean for data spaces in practice:
 IAA in data spaces	<ul style="list-style-type: none"> • What is included: overview of digital identity management procedures: Identification, Authentication, Authorisation with examples in practice. • How is it relevant: IAA is part of the building blocks necessary for the development of a data space.
 eIDAS revision	<ul style="list-style-type: none"> • What is included: overview of eIDAS1, and eIDAS2, and revision timelines. • How is it relevant: data spaces need to be aware what is on the horizon.
 EDIW	<ul style="list-style-type: none"> • What is included: overview of EDIW functionality and usability. • How is it relevant: EDIWs can be leveraged by data spaces to overcome identity related challenges.

Graph 1.0 Chapter structure overview

1.1 Digital Identity is an important building block for data spaces

Identification, Authentication and Authorisation (IAA) are highly relevant for almost any online transaction in a data space. That is because they form the basis for the digital identity management of participants, allowing them to request and send data in a trusted manner within a data space.

To illustrate, a manufacturer needs to be sure that it is the right subcontractor who is requesting the classified product data, a doctor needs to be sure that it is the assigned caretaker who is requesting the patients' treatment record, an energy provider needs to make sure the person establishing an energy contract lives at the provided address. Examples are available in almost any industry, as the table 1.1a highlights below.

Non-exhaustive

Data space	Sector	Example use case	IAA facilitates a use case
	Logistics	Export contractor needs to be sure it is the custom authority requesting access to the shipment data (e.g. freight data)	Custom authority is authorised and after authentication can access shipment data
	Automotive	Automotive parts manufacturer needs to be sure it is the right end-product assembly requesting product data & pricing lists	The end-product assembly has an access token for automated authentication
	Construction	A manufacturer needs to be sure that it is the right subcontractor who is requesting the classified buildings' data	A subcontractor authenticates themselves to get an entry to a buildings' data base
	Housing/ Real estate	A real estate agent needs to be sure it is the new owner of the house who provides a bank guarantee for a house deposit	An applicant for a house logs in to submit required documents
	Agriculture	The aggregation drone supplier needs to be sure it is the right farmer requesting crop growth data from specific fields	A farmer authenticates themselves to gain access to his crop growth data
	Energy	An energy provider needs to make sure the person with the energy contract lives at the indicated address	A homeowner authenticates themselves to see their energy bill data
	Healthcare	A doctor needs to be sure that it is the assigned caretaker who is requesting the patient's treatment record	A caretaker authenticates themselves to see their patient's treatment record
	Manufacturing	A steel facility needs to be sure that it is indeed the machine from a contracted manufacturer requesting order data	ERP system of manufacturer B has an access token for automated authentication

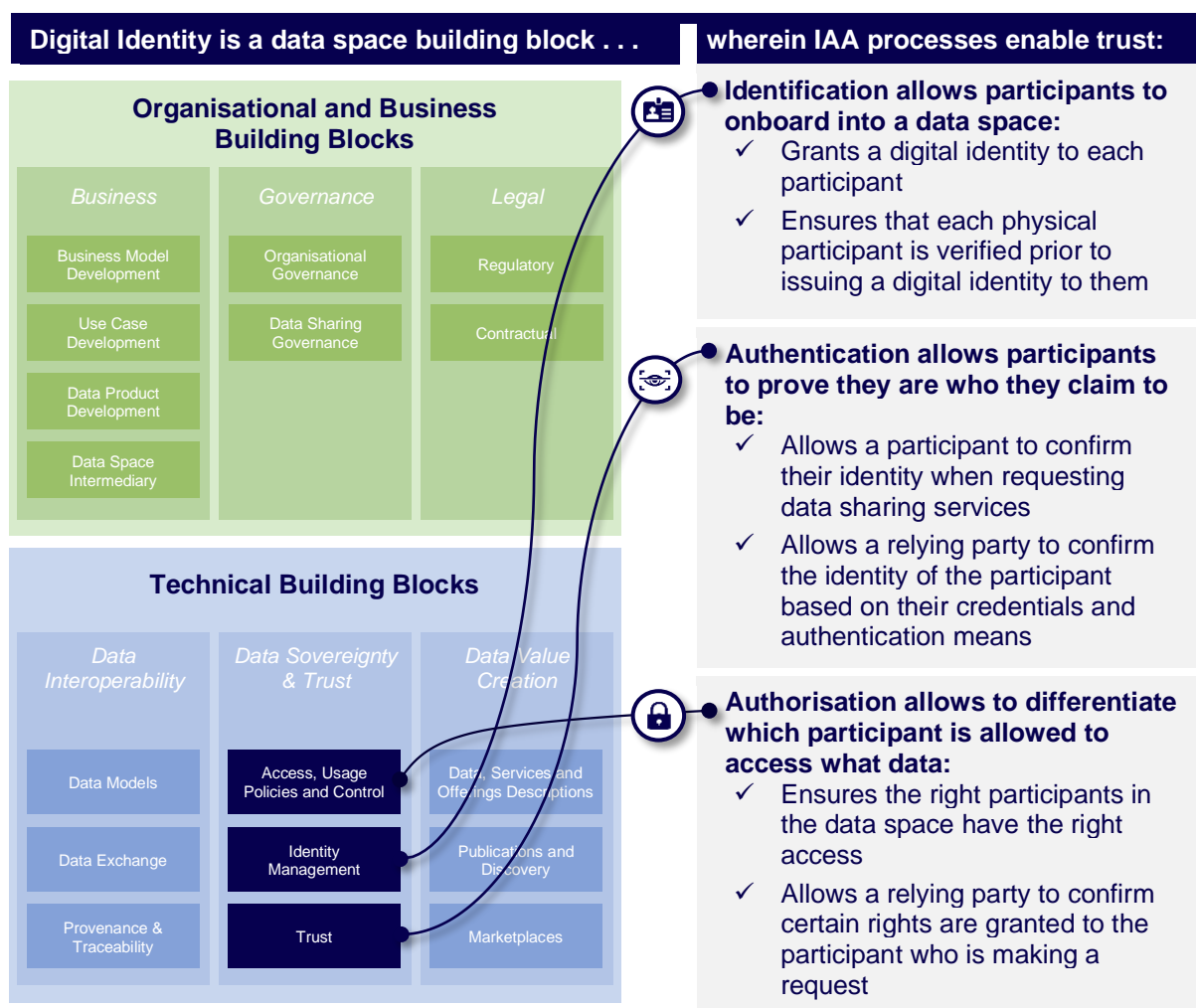
Table 1.1a Digital Identity use cases in data spaces in various industries (sectors)

These use cases illustrate the need of knowing that the right party stands behind the incoming data request, in other words having a proof that the party is who it claims to

be and are allowed to access the data. This is encapsulated in digital identity management via:

- (1) onboarding a participant to provide them with an identity (identification)
- (2) checking that a certain participant is behind the data request (authentication)
- (3) ensuring that only specific participants have access to specific data (authorisation).

Therefore, the DSSC portrays digital identity management as one of the [building blocks](#) for the data spaces development. In the CoE [DSC Data Sharing Canvas](#), IAA procedures are detailed as necessary components for that building block (see the Graph 1.1b detailing this below).



Graph 1.1b Relevance of Digital Identity for data spaces

1.2 eIDAS and its revision bring opportunities to data spaces to enhance their digital identity procedures

eIDAS1 was introduced in the EU back in 2014 to remove digital borders in Europe for identification and authentication, and to ensure security and trust for these processes. For data spaces this gives a possibility to establish regulated identification and

authentication processes that data space participants can utilise via trust service providers.

eIDAS1

eIDAS stands for electronic Identification, Authentication and Trust Services. The eIDAS Regulation establishes the framework to ensure that electronic interactions between businesses are safer, faster, and more efficient, no matter the European country they take place in. eIDAS creates one single framework for electronic identification (eID) and trust services.

eIDAS1 focuses on two important pillars: eID Schemes and Trust Services (see Graph 1.2a).



An eID allows people and businesses to manage their online affairs with a public service provider in another EEA country. They can use a national form of electronic identification (eID) recognised at European level. Recognised Dutch forms of eID are DigiD and eHerkenning. This means one can use either of these to submit your tax returns to the Austrian tax authority, for example.

Trust services under the eIDAS Regulation support businesses. eIDAS1 introduces 5 qualified (Q) trust services:

1. (Q) Electronic signature (eSignature)
2. (Q) Electronic seal (eSeal)
3. (Q) Electronic Timestamp (eTimestamp)
4. (Q) Website Authentication Certificates (WACs)
5. (Q) Electronic Registered Delivery Service (eDelivery)

Graph 1.2a eIDAS1 and the two important pillars

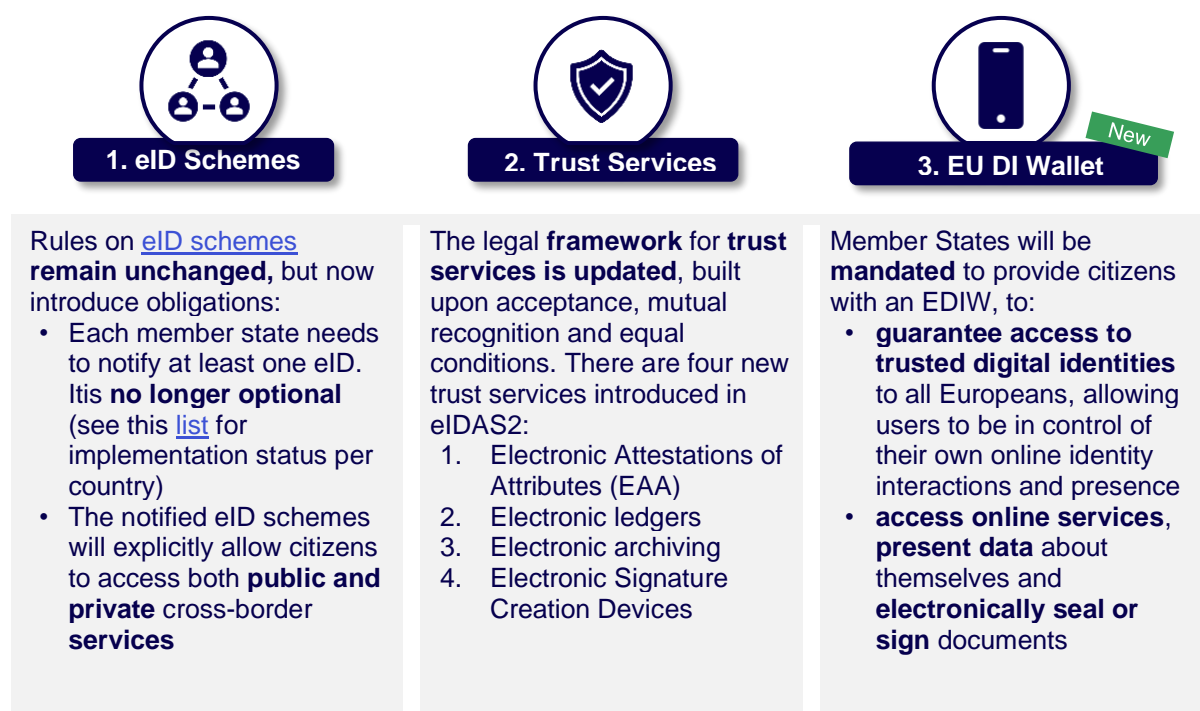
eIDAS1 is being revised to de-fragment the current European digital identity landscape and improve electronic trust services, as introduced above. Currently, this revision is being finalised.

eIDAS2 introduces new trust services and EU Digital Identity Wallets (EDIW) for the use by citizens in both public and private domains. eIDAS2 also includes Organisational Digital Identity Wallets (ODIW).

eIDAS2

eIDAS2 introduces new trust services and a privacy-preserving European Digital Identity Wallet (EDIW) to citizens and businesses, that aims to harness and build on Member States eID schemes and contain attributes issued by both public and private, qualified, and non-qualified trust service providers.

Graph 1.2b provides some of the important changes to the pillars in eIDAS2.

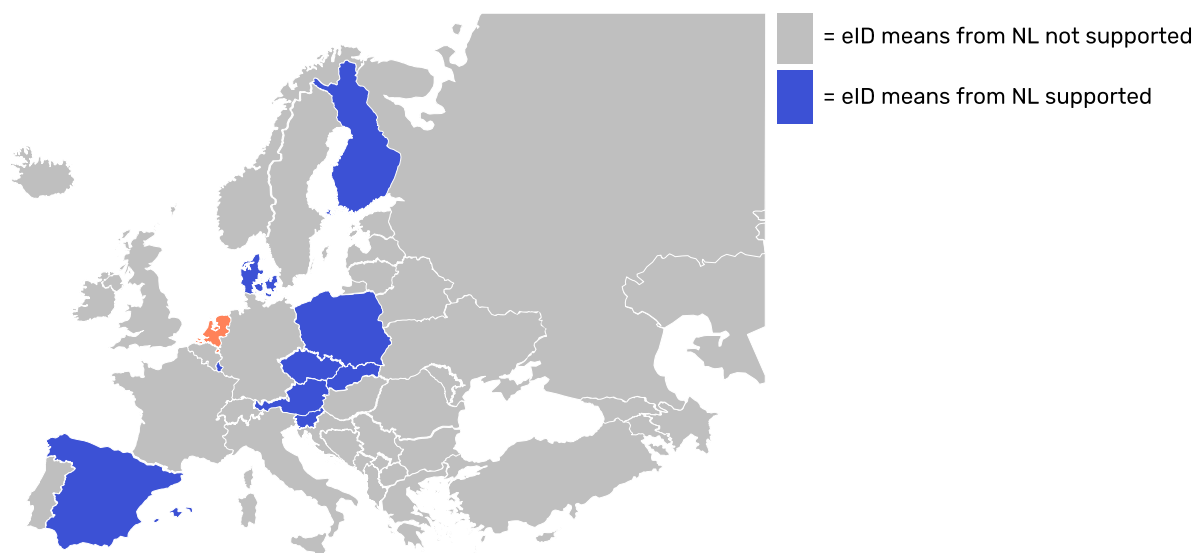


Graph 1.2b eIDAS2 and its main pillars

The legal agreement text of the eIDAS revision has been [finalised](#) following the most recent triilogue negotiations in November 2023. eIDAS2 introduces new obligations to eID schemes, additional trust services and an EU Digital Identity Wallet (EDIW). The section below elaborates on each of these introduced pillars.

For eID schemes, it becomes mandatory for member states to notify at least one eID, and accept all notified eIDs. This change improves access to public and private cross-border services, which is currently not available in and between all EU member states. For examples, Dutch citizens can only use their eID (DigiD) in the 9 EU member states as depicted in graph 1.2c³.

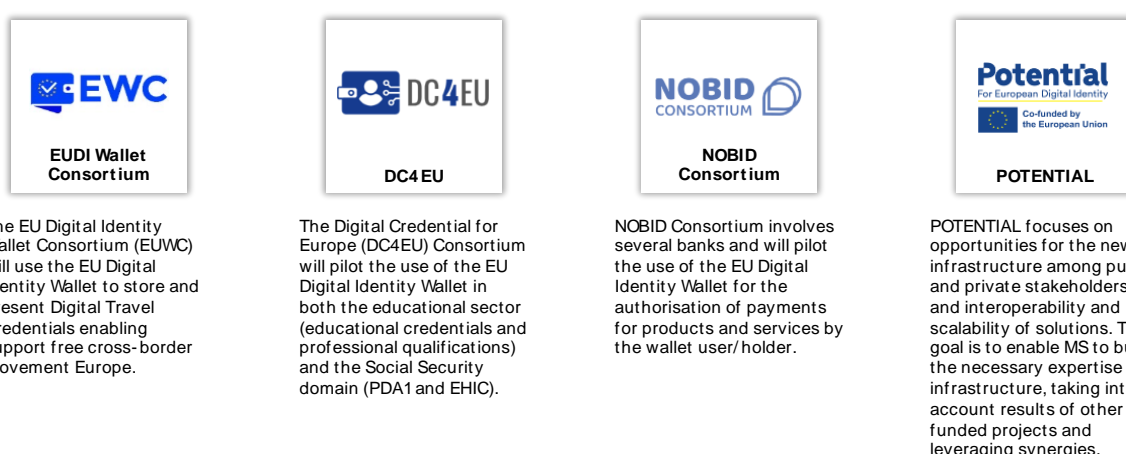
³ [eIDAS-Network](#)



Graph 1.2c Current support of the Dutch eID means among Member States

Furthermore, eIDAS2 adds four new trust services to the original list of five trust services, namely (qualified) electronic attestation of attributes, (qualified) ELedger, (qualified) EArchiving, and (qualified) management of remote eSignature and ESeal creation devices (see chapter 2 for more information on trust services).

eIDAS2 mandates the issuance of EU Digital Identity Wallets (EDIW), which are required to be rolled out in the coming 2 years in all EU Member States. The development of EDIW is supported by the Architecture Reference Framework (ARF), and a Wallet Reference Implementation, provided by the European Commission. Four Large Scale Pilots (LSPs) are currently piloting and testing elements related to the development of the EDIW⁴. More information on which use cases are being explored by the LSPs in which member state can be found on the website of the European Commission⁵. See graph 1.2d for the summary overview.

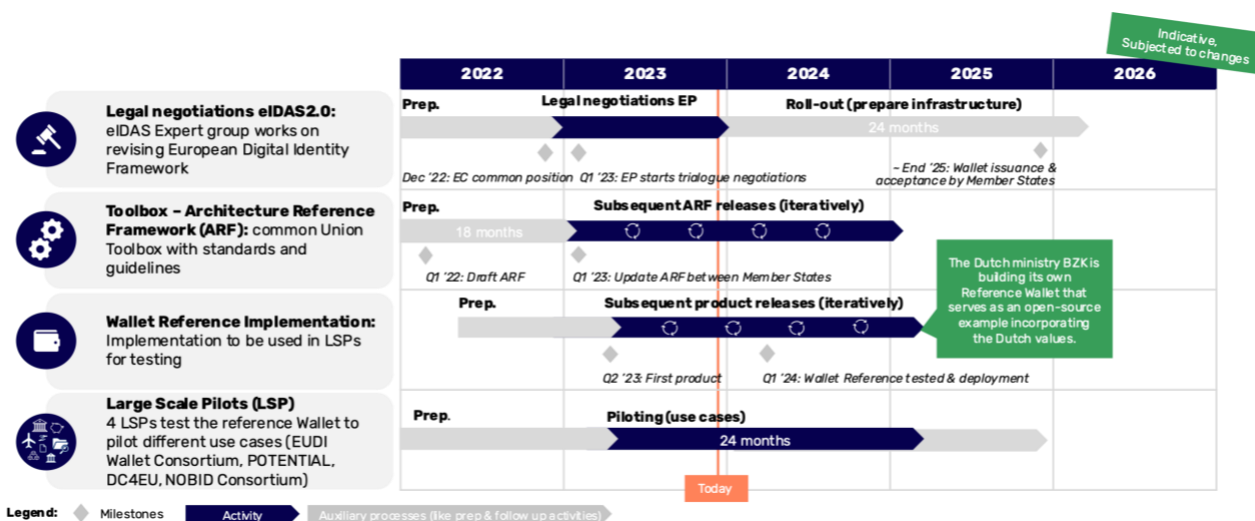


Graph 1.2d Descriptions of Large Scale Pilots

⁴ [EWC](#), [DC4EU](#), [NOBID Consortium](#), [POTENTIAL](#)

⁵ [European Commission](#)

Since the text of eIDAS2 is (almost) finalised, a phase starts where many (35-40) implementation acts are being created by the European Commission over the coming 6 to 12 months. The graph 1.2f below also depicts indicative timelines for the wallet and the ARF.



Graph 1.2f eIDAS revision and EU Digital Identity Wallet timeline⁶s

It is crucial to acknowledge that these timelines are subject to alterations. Due to the delay in the ARF, there is a concurrent risk of delays in the LSPs. The two-year implementation period commences following the publication of the final text, which is anticipated to be released in the first quarter of 2024. This timing would extend the issuance deadline of EDIWs to the first quarter of 2026. Each member state has 3 options for EUDI Wallet issuance: government-operated, outsourced or an accreditation system for private wallets. Presently, the Netherlands is inclined towards adopting an accreditation system designed to permit private wallets, though there remains ambiguity surrounding this approach.

1.3 The introduction of EDIWs brings new opportunities to many sectors

Under the eIDAS revision, EDIWs are designed to cover the usage for natural persons and legal entities, making it suitable for adoption in data spaces active in B2C, B2B and B2G contexts. To illustrate, the EDIWs main goal is to enable holders to share information obtained from issuers (providers of Electronic Attestations of Attributes) with various verifiers (relying parties). In the context of data spaces this can be interpreted as follows:

- **Natural person vs legal entity.** There is a distinction between the wallets for a natural person and a legal entity. To clarify this distinction, imagine an individual acting on behalf of themselves. This person would use the EDIW. Secondly, there

⁶ [European Commission Recommendation on common Union Toolbox](#)

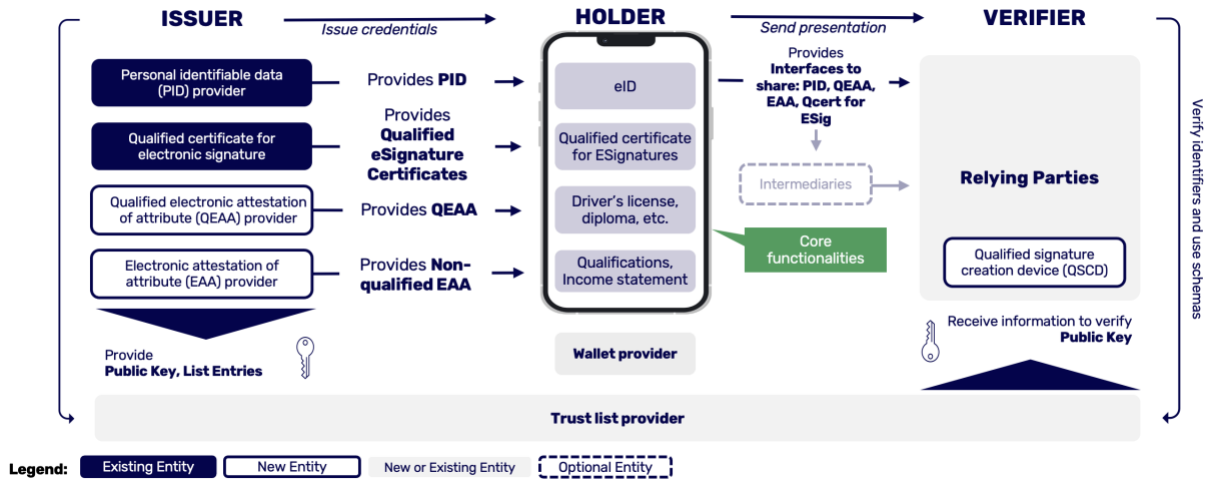
is an individual acting on behalf of a legal entity. This person would likely also use the EDIW. Lastly, there is an Organisational Digital Identity wallet (ODIW) that allows an organisation to store information about itself. To illustrate, the ODIW of a Company XYZ can contain an attribute saying that XYZ is ISO certified. This is different from the second variant mentioned above. In this second example, the CEO of Company XYZ, can have an attribute in their own EDIW, stating their role at Company XYZ. For more information on the distinction between a natural person and a legal entity in data spaces consult the model from the EU eSSIF-Lab⁷.

- **The holder** of the wallet can be a natural person, a natural person acting on behalf of an organisation, or a legal entity (in the case of a legal entity wallet), who keeps their eID (electronic ID) and various Electronic Attestations of Attributes (EAAs) in their wallet on some device. The wallet can also hold (qualified) eSignature certificates (for users) or ESeal certificates (for legal entities).
- **The issuer of (Q)EAAs** is an entity responsible for providing (Q)EAAs to the holder. In the case of qualified services, this role is performed by a Qualified Trust Service Provider (QTSP) as registered on the eIDAS Dashboard⁸. Typically, there is data space specific data and credentials that should be considered as EAA (examples). For an EAA to be valuable to a verifier, the issuer must adhere to the verifier's specific requirements. When the issuer's compliance with a verifier's requirements within an ecosystem can be confirmed, that issuer becomes a trusted entity within that ecosystem. Notably, trusted issuers of EAAs are not required to be part of the data space itself. For example, the issuer of a Personal Identification Document (PID) is recognised as a trusted source for identification information but typically is not integrated into most data spaces.
- **The verifier (relying party)** is a participant in a data space who needs to verify certain (Q)EAA. E.g.: that the holder of the wallet is allowed to access certain data, and/or be granted a certain service (in a broad sense of a service: e.g., access to age restricted goods, voting, driving a car). The verifier relies on correctness of the information encoded in the wallet regarding the holder's identity, and thus is considered to be a relying party.

Graph 1.3a schematically summarises the wallet design and its usage.

⁷ [eSSIF-Lab](#)

⁸ [eIDAS Dashboard](#)



Graph 1.3a EU Digital Identity Wallet in practice⁹

The table 1.3b below depicts some non-exhaustive examples that are being explored by the LSPs¹⁰:

PUBLIC SERVICES		FINANCIAL SERVICES	
Requesting birth certificates, medical certificates, reporting a change of address		Opening a bank account	
MOBILITY		HEALTHCARE	
Renting a car using a digital driving licence		Storing a medical prescription that can be used anywhere in Europe	
AGE RESTRICTED GOODS		EDUCATION	
Proving your age at a counter or while shopping online		Applying for a university, at home or in another Member State	
GOVERNMENTAL SERVICES		HOSPITALITY	
Filling tax returns		Checking into a hotel	

Table 1.3b non-exhaustive use cases LSPs work on

1.4 Organisations in data spaces might face mandatory acceptance of the EDIW

The mandatory acceptance of the EDIW both in public and private sectors enables a wide variety of use cases. It is mandatory for the following private relying parties to accept the use of the EDIW when strong user authentication is required by EU or

⁹ Note: QEAs shall be extracted from authentic sources

¹⁰ Note that these examples may not inherently require mandatory acceptance of the EDIW.

national law or by contractual obligation for online identification: transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, telecommunications, and education¹¹.

Furthermore, Very Large Online Platforms (VLOPs) designated under the Digital Services Act and private services that are legally required to authenticate their users will have to accept the EDIW for logging into their online services¹². The EDIW can be used to log into services from the following platforms (see table 1.4a)

Very Large Online Platforms	
▪ Alibaba AliExpress	▪ LinkedIn
▪ Amazon Store	▪ Pinterest
▪ Apple AppStore	▪ Snapchat
▪ Booking.com	▪ TikTok
▪ Facebook	▪ Twitter
▪ Google Play	▪ Wikipedia
▪ Google Maps	▪ YouTube
▪ Google Shopping	▪ Zalando
▪ Instagram	

Table 1.4a Very Large Online Platforms in accordance with EU Data Act

1.5 The introduction of EDIWs introduces new opportunities to data spaces

CoE DSC anticipates that the EDIW can offer 2 opportunities for data spaces to enhance their digital identity management, by enabling data space participants to (1) be issuers, and (2) be verifiers (see graph 1.5a below).

Data Space Opportunities for Issuing:

Data spaces can enable participants to start issuing (qualified) electronic attestations of attributes.

Non-exhaustive examples:

- Medical certificates,
- Crane operator licenses,
- Employee cards (i.e., 'A is an employee at the company XYZ')

1

Data Space Opportunities for Verifying:

Data spaces can enable participants to start verifying data from holders. Non-exhaustive examples:

- Verifying that the worker has required qualifications (e.g., of a medical professional, of a crane operator etc.)
- Verifying human representatives of a legal entity ('A indeed is an employee at the company XYZ')

2

Graph 1.5a Opportunities for Data Spaces from EU Digital Identity Wallets

¹¹ [eIDAS revision November 2023](#)







¹² [European Commission](#)

1.6 Wallets create possibilities to aid with challenges in different sectors and allow data space participants to delegate access more easily

Data spaces can generally use wallets for onboarding processes and access management for data sources (i.e., specifications of delegated entitlements to certain data at a certain source). Non-exhaustive examples include:

- A patient as a holder of a wallet, can have access to their hospital data but can also delegate data access to others, who may act on their behalf.
- A construction company as a holder of a wallet, can include construction site data they have in their repository, with described (delegated) access rights for their subcontractors.

To provide practical illustrations of the potential benefits of EDIW, Table 1.6a below highlights various challenges within data spaces across different sectors that can be mitigated by the EDIW.

Data space	Sector	Challenge(s)	Description how the EDIW addresses the challenge(s)
	Logistics	<ul style="list-style-type: none"> • Ensuring that an importer of goods has paid a tax duty at customs 	<ul style="list-style-type: none"> • An attestation with a proof of successful tax payment
	Automotive	<ul style="list-style-type: none"> • Ensuring that a supplier of machine parts (e.g. metal screws) is ISO-certified 	<ul style="list-style-type: none"> • An attestation to check ISO-certification of a supplier
	Construction	<ul style="list-style-type: none"> • Ensuring that a qualified party is contracted • Ensuring access of only authorised subcontractors to the classified facility 	<ul style="list-style-type: none"> • An attestation to check for hiring/tender illegibility • An attestation in combination with ID allow for the facility access
	Housing/ Real estate	<ul style="list-style-type: none"> • Ensuring that a new buyer has a bank guarantee for purchasing the property 	<ul style="list-style-type: none"> • An attestation from a bank and a notary of eligibility of a buyer
	Agriculture	<ul style="list-style-type: none"> • Ensuring that a chemical provider for irrigation is sustainable, e.g. having a Rainforest Alliance badge and a B-Corp rating 	<ul style="list-style-type: none"> • An attestation to check sustainability certifications of a chemical provider
	Energy	<ul style="list-style-type: none"> • Ensuring energy bills are sent to the property owner 	<ul style="list-style-type: none"> • An attestation to prove the property ownership to receive the energy readings and bills

Non-exhaustive & Indicative



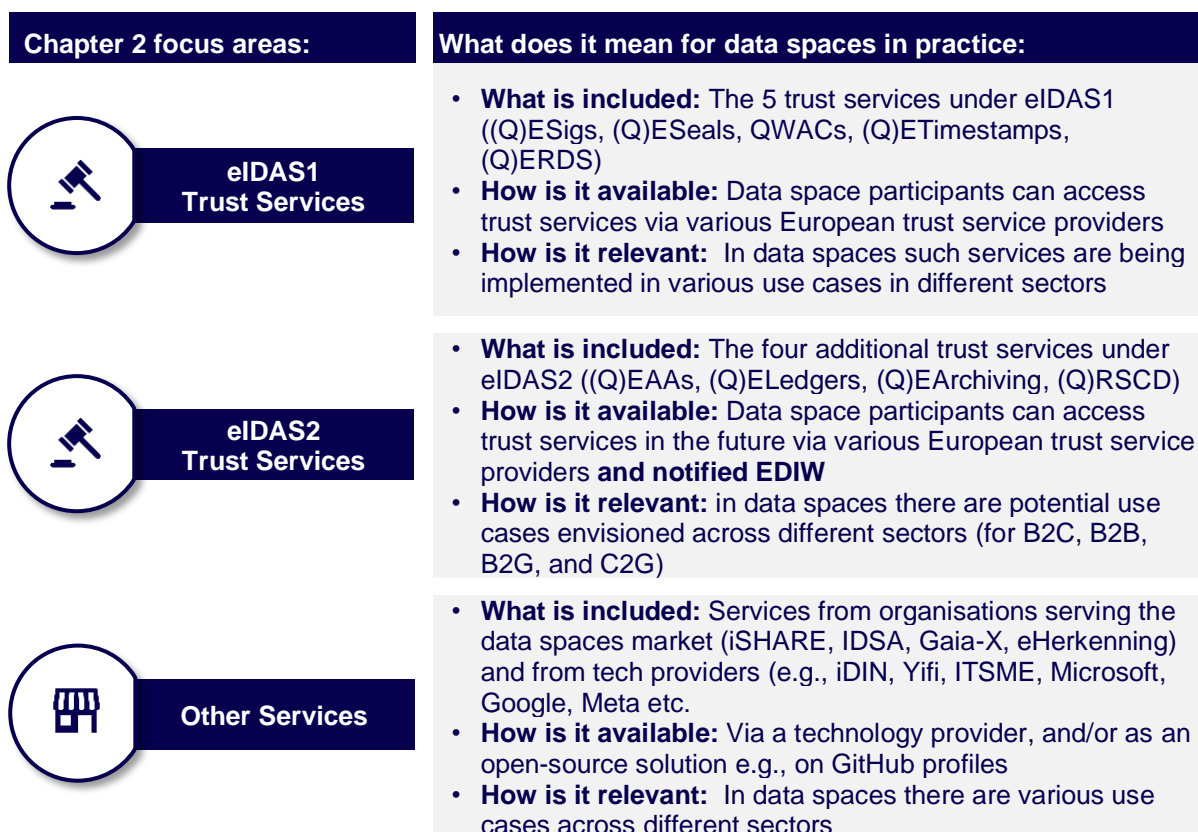
Healthcare	<ul style="list-style-type: none"> Ensuring that the assigned caretaker has access to the patient's data 	<ul style="list-style-type: none"> An attestation in a caretaker's natural persons wallet proving they can act on behalf of the patient
Manufacturing	<ul style="list-style-type: none"> Ensuring that a steel manufacturer is ISO-certified 	<ul style="list-style-type: none"> An attestation to check ISO-certification of a manufacturer

Table 1.6a Challenges that EU Digital Identity Wallets can address in different data spaces

Chapter 2. Market perspective

What is the state of the EU DI market landscape and what does it bring for data spaces?

This chapter examines the current landscape of the EU DI market by covering trust services and respective trust service providers. Hereunder is an overview of services that data space participants can leverage. This includes trust services under eIDAS1, new eIDAS2 trust services, and other services.



Graph 2.0 Chapter 2 structure overview

2.1 eIDAS trust services support trustworthy data sharing in data spaces

When conducting transactions in data spaces, it is crucial for relying parties to be certain of the legitimacy of claims made by other participants. Trust services, as outlined under eIDAS, provide this legitimacy. They offer trusted methods to securely link the content of a message to its sender or receiver. This is similar to how physical signatures or seals on a document, such as at the end of a contract or letter, establish authenticity and agreement. Examples include digitally signing a data request or sealing a digital document, which are legally equivalent to their analogue counterparts.

The eIDAS legal framework for trust services is built upon acceptance, mutual recognition and equal conditions, which means that (Qualified) Trusted Service Providers across the EU must consistently offer those services. As such, the eIDAS Dashboard serves as an overview that helps navigate for those who plan to obtain

these services¹³. In the following sections, this paper covers services under eIDAS1 and eIDAS2, as well as accompanying (potential) use cases for various data spaces.

2.2 Trust services under eIDAS1 help existing data spaces

eIDAS1 introduced five main trust service categories that improve security and trust in Europe. See Graph 2.2a for the full overview below.

Qualified Electronic Signatures	Qualified Electronic Seals	Qualified Certificates for Website Authentication	Qualified Electronic Time Stamp	Qualified Electronic Registered Delivery Service
QESigs	QESeals	QWAC	QETimestamp	QERDS
<ol style="list-style-type: none"> 1. Issuing e-signature certificates 2. Validating e-signature certificates 3. Creating e-signatures 4. Validating e-signatures 5. Preserving e-signatures or e-signature certificates 	<ol style="list-style-type: none"> 1. Issuing certificates for ESeals 2. Validating ESeal certificates 3. Creating ESeals 4. Validating ESeals 5. Preserving ESeals or certificates for ESeals 	<ol style="list-style-type: none"> 1. Issuing QWACs 2. Validating QWACs 	<ol style="list-style-type: none"> 1. Creating QETimestamps 2. Validating QETimestamps 	<ol style="list-style-type: none"> 1. Provision of electronic registered delivery services (RDS) 2. Validation of data sent via (RDS)

Graph 2.2a Overview of eIDAS1 trust services

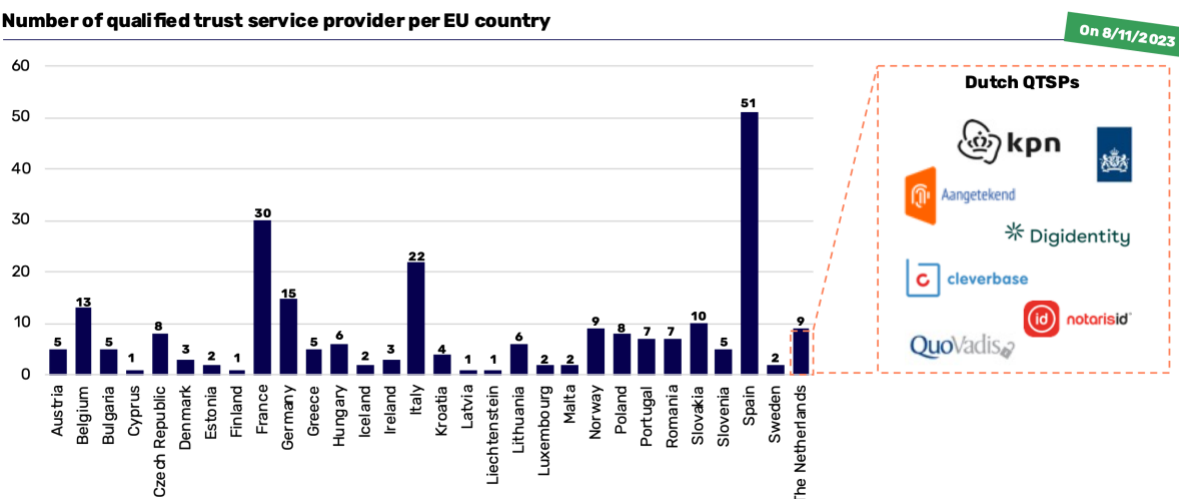
The trust services categories are described below:

1. **QESigs:** The expression in an electronic format of a person’s agreement to the content of a document or set of data. Qualified eSignatures have the same legal effect as handwritten signatures.
2. **QESeals:** Similar in its function to the traditional business stamp. It can be applied to an electronic document to guarantee the origin and integrity of a document.
3. **QWACs:** Electronic certificates that prove to your customers that your website is trustworthy and reliable. They ensure that the website is linked to the person to whom the certificate is issued. They also help avoid data phishing.
4. **QETimestamps:** Links an electronic document, such as a purchase order, to a particular time, providing evidence that the document existed at that time.
5. **QERDS:** Allows the user to send data electronically. It provides proof of sending and delivery of the document and protects companies against risk of loss, theft, damage or unauthorised alterations.

Existing trust services are available across Europe through various QTSPs for data spaces to leverage. The below graph 2.2b illustrate this in more detail:

¹³ [eIDAS Dashboard](#)

Number of qualified trust service provider per EU country



Graph 2.2b Overview of QTSPs providing services in EU with details on Dutch QTSPs¹⁴

eIDAS1 trust services are currently being leveraged by data spaces in practice to improve trust between data space participants (see the examples below).

QESigs are used to ensure proper security and authentication of natural persons sending data in data spaces

QESigs are tools for natural persons. In practice, they can be used by for example self-employed professionals involved in data spaces. An independent auditor can use QESig to sign the accounting reports to ensure non-repudiation of the contents, and supply proof that they have completed a check (example based on practices in [SBR Nexus](#)). A notary clerk can use QESig to sign the translation of the foreign contract between two parties, to ensure non-repudiation of the contents and as a proof that the contract translation has officially been made by the notary clerk in question. In a similar way in the mortgage sector the transfer of the property can be signed/sealed with QESig and QESeals (for example [HDN](#) data space participants can rely on Cleverbase as a QTSP for such processes with high level of assurance).

QESeals and QWACs are used to ensure proper security and authentication in a data space between participants

In data space “Digitaal Stelsel voor de Gebouwde Omgeving” (DSGO), QESeals are used for signing JSON Web Tokens to ensure the integrity and non-repudiation of interactions between parties (organisations) of the data space. QESeals are used in combination with QWACs, which are used to authenticate the identity of web servers and enable the confidentiality, integrity, and authenticity of communications between parties.

QESeals and QWACs are also likely going to play an important role between the EDIW and relying parties/verifiers. It is expected that data requests towards EDIWs will only

¹⁴ [eIDAS Dashboard](#)

be possible if the relying party/verifier uses QESeals and QWACs (for more details on this process see [section 2.4](#) below).

QETimestamps can be used to ensure the integrity of data at a specific time

QETimestamps record the integrity of data at a specific time, such as for an incoming patent application, creation date of a version of a document, database or software code etc. In the manufacturing sector, timestamps can be used to record when a machine got maintained. In Smart Connected Supplier Network (SCSN) timestamps are potentially useful when a record is being made on the level of degradation of an Electric Vehicle (EV) battery, which is essential to ensure transparency for future maintenance and recycling.

QERDS can be used in data spaces to share important (confidential) data

QERDS ensure that the transferred data is not tampered with when in the process of sending and receiving and safeguards against theft of the said data. In practice of SCSN, QERDS are envisioned to help when transferring sensitive documents. For example, when sharing product designs, with respective bills of materials.

2.3 Trust services under the eIDAS revision provide new opportunities for data spaces

eIDAS2 introduces four new trust services to further improve security and privacy in Europe, namely (Qualified) Electronic Attestation of Attributes (QEAA), Qualified Electronic Ledgers (QELedgers), Qualified Electronic Archiving (QEArchiving), Qualified management of remote ESignature and ESeal Creation Devices (QESCD). See graph 2.3a for the full overview below.

Qualified Electronic Attestation of Attributes	Qualified Electronic Ledger	Qualified Electronic Archiving	Management of remote ESignature and ESeal creation devices
(Q)EAA	(Q)ELedger	(Q)EArchiving	(Q)ESCD
An attestation in electronic form that allows the authentication of attributes, such as a person's nationality.	A sequence of electronic data records which should ensure their integrity and the accuracy of their chronological ordering.	A service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents to guarantee their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.	A qualified electronic signature creation device managed by a qualified trust service provider in accordance with Article 29a on behalf of the signatory.

Graph 2.3a Overview of eIDAS2 trust services

eIDAS2 trust services can be leveraged by various data spaces. Examples and descriptions are given below:

(Q)EAAs can be used for many use cases in data spaces

(Q)EAAs in combination with signatures in the wallet can enable various B2B use cases where a natural person represents an organisation, as well as B2C use cases where a natural person can gain access to the data based on the provided attributes. Some examples are:

- A variety of licenses: e.g., driver licence, crane operator licence, medical licence
- Diploma's and/or certificates: e.g., for a natural person (e.g. university programme diplomas, language diplomas, certificates of course completions, mandate to act on behalf of someone, etc.), for a legal entity (e.g. Legal Entity Identifier, ISO certification; UBO statements, registered decision makers, etc.).
- Official proofs: e.g., proofs of marriage, disability, unemployment, etc.

(Q)ELedger

(Q)ELedger services can enhance traceability of data exchanges that took place between parties. This is relevant for data spaces where sequential data exchanges occur and need to be monitored. A typical general application for (Q)ELedgers is checking the validity of (Q)EAAs. E.g. whether a certificate (driving license) is still valid or has been revoked. In the energy sector, a data space might use (Q)ELedgers as a storage for revocations to keep track of energy data access permissions and revocations (e.g., a property owner changes, a contract is made with a different energy supplier).

(Q)EArchiving

(Q)EArchiving services can allow for better management of documents over the years in the repositories of data spaces. EArchiving helps organisations with storing documents securely and safely against modifications. For documents such as property deeds, it is crucial that they are secured against unwanted modification.

(Q)ESCD

Remote (Qualified) Electronic Signature Creation Devices would ease the usage for signatures and seals for parties in the data space. This will likely be used in combination with the EDIW, because not everyone has a mobile phone that has a secure element that can contain the certificate for QESigs. The use of remote QESCDs allows citizens to sign using different devices (such as phones, laptops and tablets) regardless of whether their device has a 'Secure Element', as the certificate is stored in the cloud.

2.4 Usage of Trust Services will be essential when working with wallets to verify both issuers and verifiers

In data spaces, trusting issuers and verifiers is imperative for wallet holders. Therefore, when sharing attributes in a data space, participants have a need to verify issuers and verifiers to ensure trust in data exchanges. This is illustrated below:

- **Trusting the issuer:** A data space participant relying on an issuer's service of creating attributes needs to be certain that this issuer is a verified trusted party. For example, a university diploma is actually issued by a trusted educational institution or educational authority.

- **Trusting the verifier:** Data space participants must be confident that any verifier requesting information is a legitimate, trustworthy entity within the data space. This requires a reliable mechanism to authenticate the verifier, thereby ensuring that sensitive information is only shared with parties who have the right to access it.

Currently we foresee two options how trust between EDIWs and Issuers and Verifiers is organised:

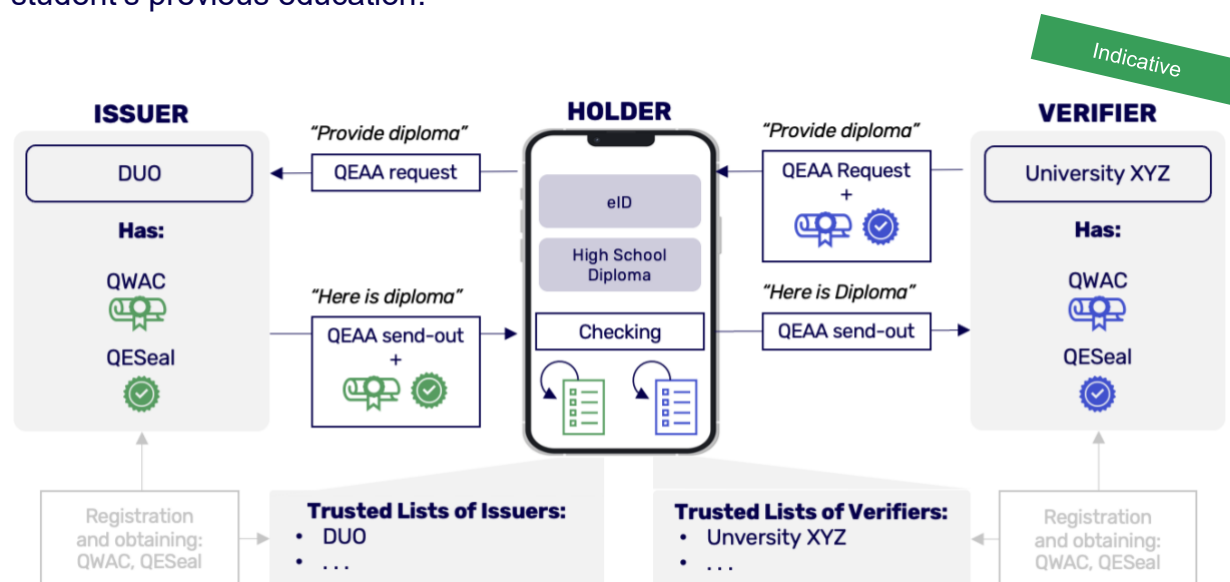
- Through using QESeals and QWACs
- Through using Decentralized Identifiers (DIDs) and (Q)ELedgers

Option A. Providing trust in issuers and verifiers with QESeals and QWACs

QESeals and QWACs can help wallets verify both the issuer and verifier to check:

- If an Issuer is trusted and/or qualified
- If a Verifier is allowed to request certain (Q)EAAs

See graph 2.4a below for an exemplary flow of a university requesting the proof of student's previous education:



Graph 2.4a A potential flow of requesting a QEAA through a EDIW

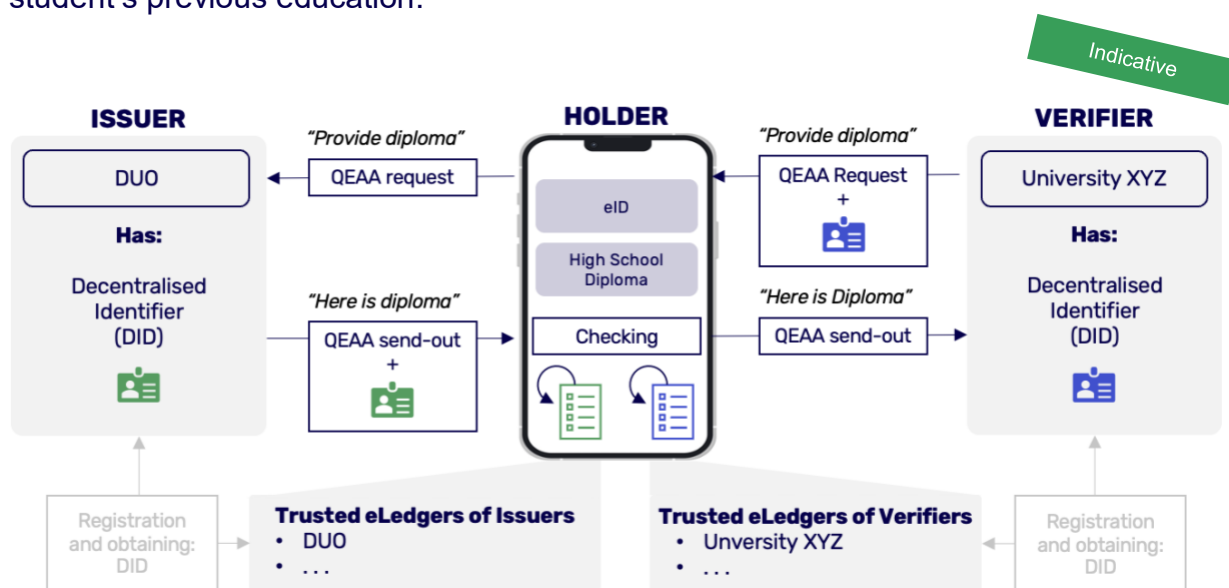
Option B. Providing trust in issuers and verifiers with DIDs and (Q)ELedgers

Alternatively, usage of Decentralized Identifiers (DIDs) and (Q)ELedgers might be implemented when working with wallets to verify both issuers and verifiers.

Decentralised Identifiers (DIDs) stored in (Q)ELedgers can help wallets verify both the issuer and verifier to check:

- If an Issuer is trusted and/or qualified
- If a Verifier is allowed to request certain (Q)EAAs

See graph 2,4b below an exemplary flow of a university requesting the proof of student's previous education:



Graph 2.4b An alternative potential flow of requesting a QEAA through a EDIW

The European Commission has not yet decided which of the two options becomes the preferred method. This decision is critical for data spaces, as it will significantly influence how they can utilise the EDIW. The decision determines whether data spaces need to invest in DIDs and (Q)ELedgers, or on QWACs and QESeals if they want to use the EDIW.

2.5 Digital identity services outside of eIDAS are also available for data spaces to leverage

Other digital identity services are also available to data spaces to improve trust. Those are offered by parties/schemes in the market like eHerkenning, iSHARE, IDSA, Gaia-X, and other more tech driven solutions (e.g., iDIN, ITSME, Yivi, Google/Apple/Meta ID), and more generic federated Identities. For more details on offerings and example usage see table 2.5a and 2.5b below:

Party	DI service description	Example(s) of usage in data spaces
-------	------------------------	------------------------------------

Non-exhaustive





	<p>iSHARE Trust Scheme, where participants can be registered in iSHARE Node by satellites & data space administrators using:</p> <ul style="list-style-type: none"> • Unique ID (EORI numbers in line with EU Identification) and • eIDAS identification and • Public keys (only for service providers and certified parties) 	<ul style="list-style-type: none"> • RVO has adopted iSHARE to boost Green Deal Data Space, allowing owners of non-residential buildings to access & share energy consumption data • The DVU (Data space for Energy Reduction in Non-Residential Buildings), through iSHARE manages access to historical energy data for CO2 reduction projects
	<p>Provides a scheme for obtaining authentication means for employees acting as legal representatives of an organisation. This scheme supports 4 assurance levels (LoA), and includes:</p> <ul style="list-style-type: none"> • eHerkenning authorised DI with authentication means • Certified Trust Service Providers 	<ul style="list-style-type: none"> • eHerkenning enables B2G transactions (e.g. in the Netherlands filing taxes on behalf of the legal entity) • eHerkenning enables B2B transactions (e.g. signing on behalf of the company one is working for)
	<p>IDS Reference Architecture Model (RAM), with open standards on GitHub. For DI management it specifies a certification scheme with 3 assurance levels (LoA), and includes:</p> <ul style="list-style-type: none"> • IDS-ID for a participant with respective certificates (X.509) • Dynamic Attribute Provisioning Service (DAPS) • Certification Body and Certification Authority 	<ul style="list-style-type: none"> • SCSN relies on IDS connectors to enable trusted exchange between steel manufactures
	<p>Supported SSI ecosystem as a part of Gaia-X Federation Services (GXFS). Consists of open standards and tools, including:</p> <ul style="list-style-type: none"> • Decentralised Identifiers (DIDs) • Verifiable Credentials (as part of Gaia-X Self Descriptions) • Organisational Credential Manager (OCM) • Gaia-X Verifiable Data Registry (VDR) 	<ul style="list-style-type: none"> • Catena X relies on GXFS services to enable trusted exchange between automotive manufacturers in the supply chain

Table 2.5a Overview of other digital identity services for B2B usage in data spaces

The table 2.5b provides an overview of various digital identity services tailored for B2C use cases, offered by tech providers:

Party	DI service description	Example(s) of usage in data spaces
-------	------------------------	------------------------------------

Non-exhaustive




<p>Scheme(s)</p> 	<p>B2C ID schemes allow a natural person to authenticate their identity</p>	<ul style="list-style-type: none"> • MFFBAS uses iDIN, to identify energy consumers when they sign an energy contract • In the real-estate sector, a buyer can sign a mortgage contract for a new property using their iDIN¹⁵ or use the Vidua Wallet • EDSN¹⁶ uses iDIN to identify consumers and companies with a small-scale connection when sharing data with grid operators.
<p>Wallet providers</p> 	<p>Wallet providers: allow natural person to authenticate themselves</p>	<ul style="list-style-type: none"> • MFFBAS partners with Yivi as a wallet provider to help with digital identity of energy consumers
<p>Tech providers</p> 	<p>Technology solutions compatible with eIDAS regulation</p>	<ul style="list-style-type: none"> • The Dutch public services project Rode Knop¹⁷ with CJIB and municipalities uses Ledger Leopard solution to help citizens apply for debt assistance • Sphereon provides an eIDAS compliant signature client¹⁸, and provides expertise on verifiable credentials as part of two LSPs (EUWC and POTENTIAL)
<p>Big Tech Platforms</p> 	<p>Identities connected to accounts obtained from big tech platforms</p>	<ul style="list-style-type: none"> • A Microsoft account can be used to login as a representative of a company e.g. to file corporate expenses • A Google account can be used to login as a natural person to access certain services, e.g. to order a product from online shop and arrange delivery options

Table 2.5b Overview of other digital identity services for B2C usage in data spaces

¹⁵ [iDIN usage examples](#)



¹⁶ [iDIN usage in EDSN](#)

¹⁷ [Rode Knop \(de nationale Pauzeknop\) project with Ledger Leopard](#)

¹⁸ [Sphereon eIDAS compliant signature client](#)

Chapter 3. Practical steps for data spaces

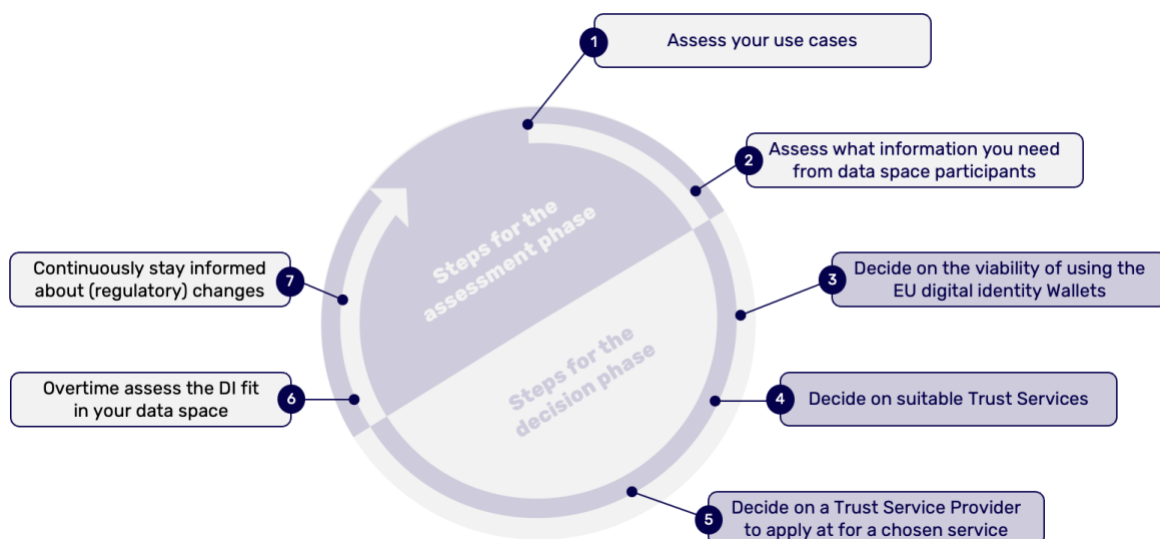
What are practical steps to implement suitable digital identity solutions in a data space in line with regulatory and market perspectives?

Chapter 3 focus areas:	What does it mean for data spaces in practice:
 <p>Roadmap for Data Spaces</p>	<ul style="list-style-type: none"> • What is included: A roadmap for getting a suitable digital identity solution in a data space. • How is it relevant: There is no one size fits all. Data spaces need to be aware of the steps to assess and implement needed solutions accordingly.
 <p>Ways to stay informed</p>	<ul style="list-style-type: none"> • What is included: Practical ways for data spaces to stay informed and join conversations on legislative changes. • How is it relevant: Data spaces need to stay informed on what digital identity legislation brings to avoid lagging behind.

Graph 3.0 Chapter structure overview

3.1 Follow a roadmap to get suitable digital identity solutions in a data space

This section covers the step-by-step actions that data spaces can take to establish suitable digital identity solution for their participants. It is important to note that there is no one-size fits all solution. Data spaces are first encouraged to assess what use cases they are working with, what is the required level of assurance for those use cases and only then determine relevant digital identity processes (e.g. suitability of wallets, suitability of trust services etc.). Overtime data spaces should continuously monitor changes and adjust digital identity processes accordingly, to ensure that participants’ needs are catered for accordingly. The graph 3.1a below illustrates a roadmap and summarises the steps to take:



Graph 3.1a Decision roadmap for data spaces

Assess data space use cases: A data space should consider what data sharing use cases should be supported. The data space should determine which partners (inside and outside of the data space) are involved and assess the risks involved. Determining the required Level of Assurance (LoA) for the use case helps deciding on appropriate DI solutions:



Explanation:

- Use cases in a data space require a certain level of assurance, depending on the nature of the use case (e.g., sensitivity of the data involved, risks from data misuse)
- Processes for identification, authentication and authorisation (IAA) provide participants with a certain level of assurance (means)
- When LoA requirements are known, a flexible matching can take place to determine what authentication mean is suitable for what use case
- Note that the weakest link of the two (identification procedure & authentication mean) determines the LoA. A strong authentication mean with a weak identification process has low assurance, just like a weak authentication mean with a strong identity proofing process.

Graph 3.1b Use case types and respective LoAs

Assess what information is needed from data space participants and external parties:

It is important for data spaces to assess what (verifiable) information is needed in the considered use case. This information can be relevant for and come from their participants and partners outside their data space.

- What data do companies need to verify?
- What data do companies need to issue?

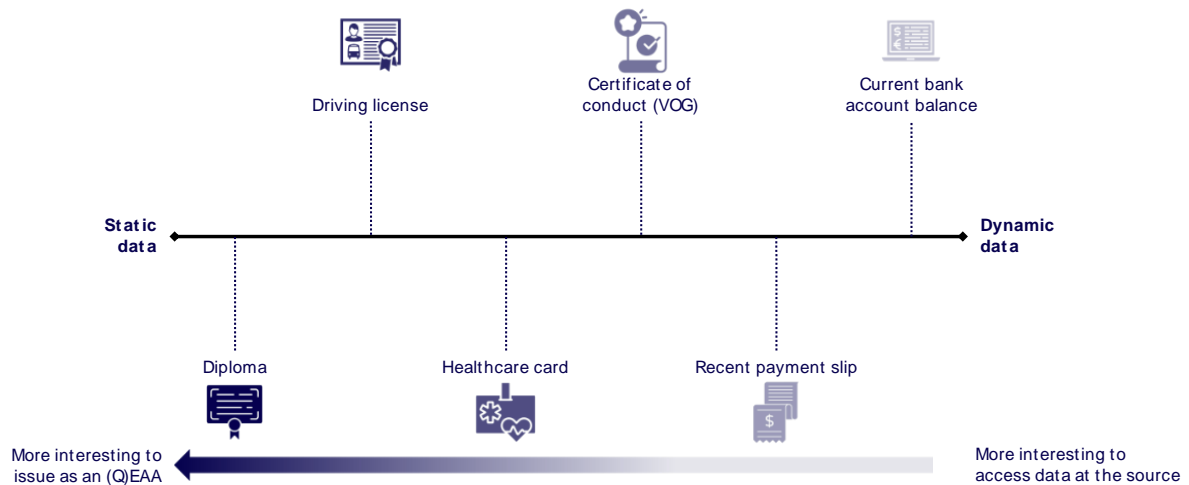
Once a data space has determined which information/data is needed, it is important to decide on whether or not to use the EDIW. Current or foreseen use of DI solutions amongst the stakeholders in information exchange can also influence this decision.

Decide on the viability of using the EDIW:

Once it is determined which information/data is required, it should be assessed whether it is suitable for organisations in the data space in question to issue the data as a (Q)EAA or to keep the data closer to the source. (Q)EAAs are particularly valuable for use cases involving static data. When data is transferred (copied) away from its original source into an EDIW, it risks becoming outdated, especially for real-time data. However, this challenge is less significant for highly static data, such as diplomas or driving licenses, which don't experience frequent changes. These types of attestations are ideal candidates to be issued as (Q)EAAs due to their static nature.

For more dynamic attestations, like a person's current bank account balance, verifiers require the most current and accurate information. An attestation from yesterday may no longer be relevant. For instance, a person may have an attestation from yesterday showing their bank account balance, but they could have spent or transferred all their money since then, rendering the attestation obsolete. For such dynamic data points,

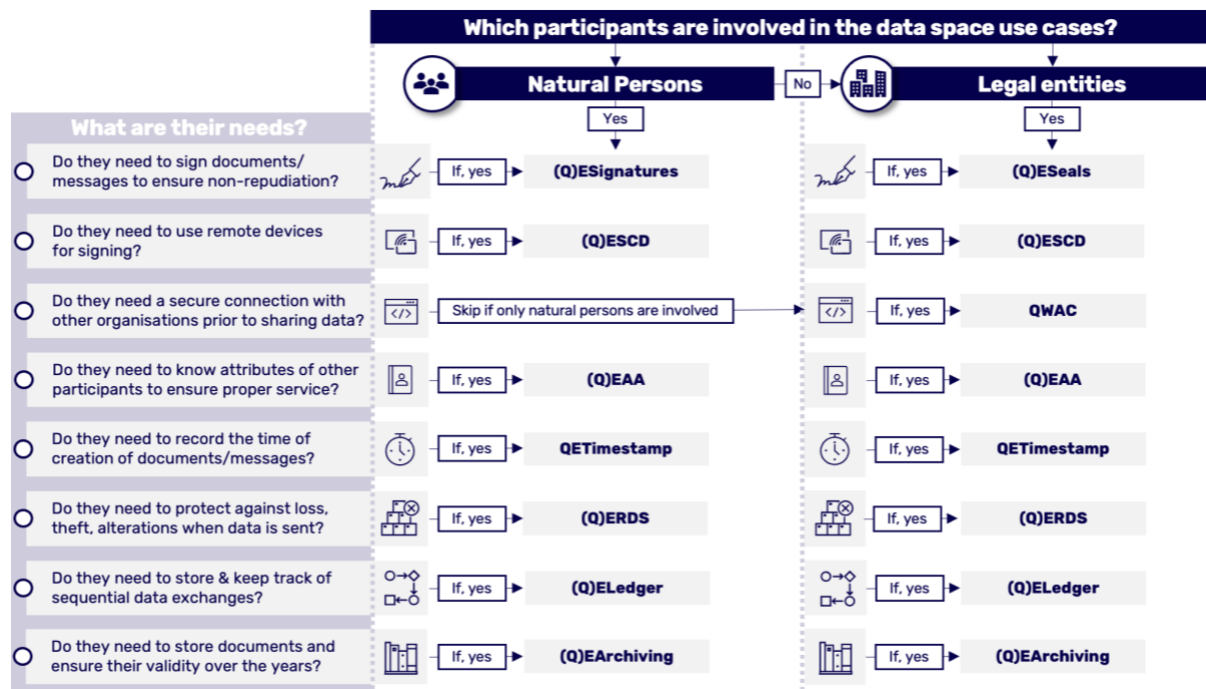
exploring alternative methods to share the data becomes more pertinent. The following figure provides a general overview of various attestations and their positioning on a scale from static to dynamic data:



Graph 3.1c Channels for data spaces to use to stay aware of regulatory developments.

Decide on suitable trust services:

Given data sharing use cases that a data space supports, decisions should be made with regards to suitable trust services to be used. You can use a flowchart checklist below to help with your decisions.



Graph 3.1d A decision flowchart for trust services

Apply at a (Qualified) Trust Service Provider:

After a data space has decided which trust services to use, the data space can request the service at a QTSP. In the Netherlands, there are currently nine Qualified Trust Service Providers that offer trust services:

QTSP's in the Netherlands	(Q)ESignatures	(Q)ESeals	(Q)WACs	(Q)ETimestamps	(Q)ERDS
Aangetekend B.V.					<input checked="" type="checkbox"/>
CIBG	<input checked="" type="checkbox"/>				
Cleverbase ID B.V.	<input checked="" type="checkbox"/>				
Digidentity B.V.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
KPN B.V.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Ministerie van Defensie	<input checked="" type="checkbox"/>				
Ministerie van Infrastructuur en Waterstaat	<input checked="" type="checkbox"/>				
NotarisID B.V.	<input checked="" type="checkbox"/>				
QuaVadis Trustlink B.V.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

= Qualified = Non-qualified

Graph 3.1e List of QTSPs in the Netherlands

It is recommended that data spaces review the eIDAS dashboard to find trust service providers that offer current and future trust services¹⁹. As of now, trust services under eIDAS2 are not yet operational. However, it is anticipated that existing QTSPs will begin offering these upcoming trust services. For data spaces interested in utilising these new trust services, it is advisable to contact current QTSPs for more information.

Additionally, for the Dutch data space participants obtaining PKI-Overheid and/or eHerkenning is often a requirement to share data in B2G and B2B settings. See appendix for summary steps on how to obtain those means.

Assess the digital identity solution compatibility continuously:

Regularly evaluate the effectiveness of the Digital Identity (DI) solution within the data space. Periodically review and adjust the suite of trust services and solutions, making decisions about which ones to adopt, continue, or discontinue based on their relevance and performance.

Actively stay informed:

Maintain an active approach to learning about new and existing services. Ensure that the data space is consistently informed about regulatory changes and industry developments. For comprehensive information and guidance, referring to the

¹⁹ [eIDAS Dashboard](#)

upcoming section 3.2, which provides detailed insights on staying abreast of these critical aspects, might help.

3.2 Practical ways for data spaces to stay informed and join conversations on legislative decision making

It is important for data spaces to stay informed on the latest developments of eIDAS2. While the legal text of eIDAS2 is (almost) finalised, the EU Commission is preparing many (35-40) implementation acts over the coming 6 to 12 months. Also, the ARF is still under development and will also be revised in 2024. For data spaces to stay informed and join the discussion, they can go through several Dutch and European channels:

Channel	Link	Description
Stakeholder platform EU eIDAS	Link	Through this platform on European Digital Identity, the European Commission aims to build a virtual community of stakeholders to provide feedback on the work of the eIDAS Expert Group on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.
Large Scale Pilot participants: Bureau LSP	Link	Bureau LSP supports Dutch organisations in participating in LSPs with the EDIW. The bureau also coordinates Dutch participation in consortium Potential.
The Dutch EDI Stelsel	Link	The central information page on European Digital Identity and the EDIW.
Decentralised Identity Interop Profile Meet-ups	Link	DIIP Meet-ups are part of the Dutch Blockchain Coalition. During the DIIP meet-ups, use cases and which features in the profile are still missing are discussed.
The Architecture Reference Framework	Link	The GitHub repository that contains the ARF.

Table 3.2a Channels for data spaces to use to stay aware of regulatory developments.

Additionally, data spaces are encouraged to join the conversions at the many events related to the topics of Digital Identity and eIDAS:

Event	Link	Description
IDNext	Link	The IDnext conference “The state of Identity” focused on all aspects of these developments, including privacy, trust, inclusiveness, data, AI, ethical, safety, social and assurance.
CoE-DSC Event	Link	The CoE-DSC aims to lower barriers and help participants realise the full potential of data sharing initiatives.

European Identity and Cloud Conference	Link	Leading event for the future of digital identities and cybersecurity
SSI meetups	Link	Quarterly meetup for all interested in the application of (Self Sovereign) Digital Identity. Organised by the DigiCampus and the Dutch Blockchain Coalition

Table 3.2b Event for data spaces to attend to stay aware of regulatory developments.

Chapter 4. Recommendations

It has become evident that the landscape of digital identity is rapidly evolving. In this dynamic environment, data spaces must adopt a strategic approach to remain agile and effective. The following recommendations are designed to guide data spaces in navigating these changes:

Engage proactively with eIDAS2: Data spaces should explore opportunities, to maximise leverage of eIDAS2 functionalities as generic building blocks and not reinvent the wheel. Depending on the data space, both in Trust Services domain and the EDIW domain eIDAS2 provides off the shelf components and infrastructure that can be reused and adapted to the data space's need. For data spaces that face mandatory acceptance of the EDIW (e.g. government, banking, utilities), implementation timelines are short. Only 24 months after the adoption of the regulation, they should accept the wallet in all their channels, so it is recommended start preparing now.

Follow the roadmap to implement suitable digital identity solutions that ensures interoperability in the long run: Data spaces should explore opportunities while building upon the foundation of eIDAS as a generic way to support digital identity processes in a future-proof and interoperable manner. Leveraging common EU-wide digital identity means allows for easier growth of a data space in terms of new participants. It also enables cross-sectoral data sharing opportunities. Data spaces can follow the roadmap presented in this whitepaper to identify suitable digital identity solutions and stay up to date with regulatory changes.

Foster collaboration and partnerships: Collaboration and partnerships in and among data spaces, digital identity providers, and regulatory bodies should be encouraged. This collaborative approach can lead to a better understanding of the practical implications of eIDAS. By working together, stakeholders can develop more innovative and efficient solutions to common challenges, share best practices, and leverage collective expertise to navigate the eIDAS landscape more effectively.

Limitations of the research and next steps

The whitepaper's recommendations emphasize the importance of aligning data spaces with eIDAS. It is essential that data spaces not only meet compliance requirements but also leverage the possibilities offered by eIDAS. This approach will improve digital identity management and security within their data space. It also paves the way for interoperability across various sectors in the future.

In that regard, further research work is needed to assess (and potentially align) the eIDAS identity management developments with the developments in the EU Data Strategy initiatives like Data Space Protocol, IDSA, Gaia-X, DSBA, DSSC-Blueprint, SIMPL.

Appendix

A. Abbreviations used

Below see the list of abbreviations (table A.1) used in the paper.

Abbreviation	Description
CoE DSC	Centre of Excellence for Data Sharing and Cloud
DI	Digital Identity
DSSC	Data Space Support Centre
eID	Electronic ID
eIDAS	EU regulation for electronic Identification, Authentication and trust Services
EDIW	European Digital Identity Wallet (refers to the EU wallet for natural persons)
IAA	Identification, Authentication, Authorisation
IDSA	International Data Spaces Association
ODIW	Organisational Digital Identity Wallet (refers to the EU wallet for legal entities)
(Q)EAA	(Qualified) electronic attestation of attribute
(Q)EArchiving	(Qualified) electronic archiving
(Q)ELedger	(Qualified) electronic ledger
(Q)ERDS	(Qualified) electronic registered delivery service
(Q)ESCD	(Qualified) electronic signing creation devices
(Q)ESeal	(Qualified) electronic seal
(Q)ESignature	(Qualified) electronic signature
(Q)ETimestamp	(Qualified) electronic timestamp
(Q)TS	(Qualified) Trust Services are services under eIDAS regulation including creation, verification, validation of various electronic digital identity means, and management of electronic signing devices
(Q)TSP	A (Qualified) Trust Service Provider is a party who provides one/or several services of creation, verification, validation (and/or device management) as part of (Qualified) Trust Services under eIDAS regulation
(Q)WAC	(Qualified) website authentication certificate
SSI	Self-Sovereign Identity
VLOPs	Very Large Online Platforms (coined in EU regulation)

Table A.1 List of used abbreviations

B. Terms used

Below see the list of terms (table B.1) used in the paper

Term	Description
Data space	A data space is a collective term for entities (i.e. both natural and legal persons) that are participating in (and/or are enabling) data exchanges by relying on some common infrastructure and pre-arranged agreements.
Data space participant(s)	Used interchangeably with a data space user. Any party that participates in a data space by either engaging in some form of a data exchange, or by facilitating the said exchanges, and who adheres to the data space agreements.
Issuer	A party who provides (qualified) electronic attestations of attributes to a holder of the digital identity wallet
Holder	A party (natural and/or legal person) who keeps their eID (electronic ID) and various Electronic Attestations of Attributes (EAAs) in their digital identity wallet on some device.
Relying party	A party who relies on the authenticity of a digital identity mean (e.g., relies on the authenticity of electronic attestation of attribute). In this paper a relying party is used interchangeably with verifier.
Verifier	A party who needs to verify authenticity of a certain digital identity mean from a holder in order to share data with them and/or provide some other service. (E.g., confirming it is the patient's doctor to give them access to the patient's dossier; confirming someone is 18+ prior to selling alcohol to them).

Table B.1 List of terminology

C. Additional information for Dutch organisations engaged in data sharing on steps to obtain PKI-Overheid and eHerkenning

In the Netherlands, obtaining PKI-Overheid Certificates and/or eHerkenning digital identity means is often a requirement to share data in the B2G and B2B settings. Below are the steps for organisations on how to obtain those means:

3 Steps to obtain PKI-overheid certificate*:

- 1 Choose your QTSP:**
- 2 Go through identification process at your QTSP:**
Submit the details for your PKI-Overheid:
 - i.e. provide EORI number*Identification of the certificate manager:*
 - The certificate manager gets an appointment for personal face-to-face identification
- 3 Receive your PKI-overheid Certificate**
 QTSP will deliver your certificate by email.

Note: * Steps may slightly vary depending on the QTSP:

Graph C.1 How to apply for a PKI-Overheid Certificate

Apply at one of the 6 eHerkenning trusted certified suppliers to obtain eHerkenning means

Steps 1-3 cover decisions for applying for eHerkenning
Steps 4-6 describe the actions for obtaining eHerkenning

<p>Step 1:</p> <p>Decide on service providers you want to log into</p> <p>More than 500 different service providers (i.e. governmental and private organizations) allow you to login with eHerkenning.</p> <p>Check this list to see which service providers you intend to connect to with eHerkenning.</p>	<p>Step 2:</p> <p>Decide who will represent the company using eHerkenning</p> <p>Single eHerkenning means with the accompanying authorisations are linked to one individual only.</p> <p>You need to issue eHerkenning means individually for each representative. But it is possible to apply for them in bulk.</p>	<p>Step 3:</p> <p>Decide on the needed level of assurance out of 4 levels:</p> <p>EH2 EH2+ EH3 EH4</p> <p>The service provider determines the LoA required for their online services.</p> <p>If you intend to use multiple services, better opt for the highest level.*</p> <p><small>*Note: if needed the level can be upgraded later on</small></p>								
<p>Step 4:</p> <p>Authorise each individual representative</p> <p>The authorisation specifies for which service providers, and for which services, an individual can log into on behalf of their organisation.</p> <p>Two people grant an authorisation: Authorised signatory Authorisation manager</p>	<p>Step 5:</p> <p>Select a trusted supplier and apply for eHerkenning</p> <p>6 official suppliers of eHerkenning can identify you and provide login means based on the assurance level you choose.</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>	<p>Step 6:</p> <p>Activate eHerkenning means and start using them</p> <p>Once you have purchased eHerkenning login means*, you can activate and use them.</p> <p><small>*Overview of login means per assurance level:</small></p> <table style="font-size: small; border-collapse: collapse;"> <tr> <td style="background-color: #e91e63; color: white; padding: 2px;">EH2</td> <td>Username & password</td> </tr> <tr> <td style="background-color: #e91e63; color: white; padding: 2px;">EH2+</td> <td>2FA</td> </tr> <tr> <td style="background-color: #e91e63; color: white; padding: 2px;">EH3</td> <td>2FA</td> </tr> <tr> <td style="background-color: #e91e63; color: white; padding: 2px;">EH4</td> <td>PKI certificate or 2FA</td> </tr> </table>	EH2	Username & password	EH2+	2FA	EH3	2FA	EH4	PKI certificate or 2FA
EH2	Username & password									
EH2+	2FA									
EH3	2FA									
EH4	PKI certificate or 2FA									

Graph C.2 How to apply for eHerkenning digital identity means²⁰

²⁰ [eHerkenning](#)