



# Identity assurance in growing data sharing networks

SCSN's case study

# Management Summary – Introduction



## Introduction

- SCSN is a growing data space for the manufacturing industry with participants ranging from larger OEMs and first-tier suppliers, to SME second- and third-tier suppliers, wholesalers and steel manufacturers (>300 user base).
- Through SCSN, users can share data through their IT system provider on a peer-to-peer basis.
- SCSN has growth ambitions (a.o., scope, users, geographical) that will increase value potential for users, but in parallel also increase the associated risks involved in peer-to-peer data sharing.
- The following **3 key risks in growing data sharing networks** were identified:
  - 1. Financial** - A risk that is incurred by a data sharing participant in case of fraud. It involves potential loss of cash and/or other liquid assets, as well as loss and damage of tangible assets like raw material, inventory and equipment.
  - 2. Compliance** - A risk that is incurred by a data sharing participant which involves exposure to legal penalties due to non-compliance to industry laws and regulations, and internal policies or clauses within contracts.
  - 3. Reputational** - A risk that is incurred by a data sharing participant which involves reputational damage to the company brand due to mis-use of digital identity or fraudulent actions during data sharing.
- To mitigate associated risks, SCSN is rethinking digital identity assurance of their end-users and has requested DSC's help to provide strategic input for their Levels of Assurance framework.
- With the insights generated by the case study, DSC can also support other data spaces in developing digital identity assurance.

# Management Summary – Key Findings



## Key Findings for building SCSN LoA Framework

Based on the desk research and interviews with SCSN stakeholders **seven key findings** related to the development of the framework were identified.

1. Risks related to digital identity assurance in SCSN are **driven by 3 factors**: (1) the scope of messages supported by SCSN, (2) SCSN's geographical scope of operations and (3) the size of adoption in terms of scale of the network.
2. Higher levels of identity assurance are required **once a data initiative starts to expand** users and facilitate new use-cases, thence data sharing becomes more complex and risky (e.g., reputational, financial, compliance)
3. SCSN should improve measures in 3 key areas: **identification, authentication and risk-mitigating policies**. Hereunder, the identity assurance solutions are referred to as identification and authentication procedures. Other policies include peer-review processes, monitoring policies and liability contracts between SCSN foundation and SPs. (For detailed explanation of terminology, please, refer to page 9 of this document).
4. Identity assurance procedures to join the network need to be carried out in the **uniform fashion among participants** of a data initiative to avoid friction and misaligned expectations.
5. When user groups in a data sharing initiative have different trust requirements and implementation capabilities, **several levels of assurance should be supported** (e.g. basic and plus levels) to stimulate adoption among all user groups. In SCSN's case, lower LoA with base requirements are needed to satisfy small SMEs using SCSN, while higher LoA for the use of advanced SCSN messages will cover the needs of the 'corporate' users.
6. SCSN as a growing data initiative is advised to **move towards eIDAS certification** for identification and authentication of their participants. That is because identity assurance means regulated under the eIDAS allow for future scalability and higher assurance. Moreover, eIDAS means like certificates for qualified electronic seals (QESeals) are becoming widely adopted in various other sectors (e.g. financial (SBR Nexus), logistics (iShare)), and can be re-used by SCSN to improve the procedures, as SPs can rely on trusted 3rd parties for user authentication.
7. The implementation of the LoA framework should be carried out in a **phased manner** in order to prepare participants for the change, and to carry out iterative peer-review process to assess the fit between risks and trust of the solutions and make improvements accordingly.

# Management Summary – Proposed LoA framework and Roadmap



## Proposed SCSN LoA framework

Based on the findings, LoA framework that effectively addresses users' needs includes at least 2 assurance levels (base and plus) and additional policies to mitigate risks:

- **Base Level assurance** consists of identification and authentication measures that satisfy less tech-savvy user group (e.g. conducting checks of their bank account and chamber of commerce registration, and issuing 2FA means to log into the SP environment).
- **Plus Level assurance** consists of identification and authentication measures that satisfy users of more advanced SCSN messages (e.g. besides conducting basic checks require users to obtain GLN number on their own and purchase eIDAS QESeals for authentication).
- **Additional policies** include peer reviews, monitoring policies and liability contracts that can be part of the additional risk-mitigating measures to improve trust. They are needed to ensure aligned development and implementation of LoA framework and instil mechanisms to timely detect and resolve digital identity mis-use.



## High level Roadmap for Execution

DSC developed a three-stage roadmap to improve LoA framework and stimulate adoption throughout different growth phases of the network:

- **Stage 1 – implement Base.** A network should focus on establishing unified Onboarding Policy across all SPs and set up the peer-review process in order to avoid misaligned expectations and identify common agreed upon solutions for Base and Plus levels of assurance.
- **Stage 2 – implement Plus.** After unified onboarding is in place, the network should set up user-to-user assurance solution wherein users can be identified and authenticated through digital certificates under eIDAS. Thus, assurance in the user identity is handled in uniform manner as SPs can rely on Trusted 3rd parties for user authentication.
- **Stage 3 – implement additional means.** In the long run the network should consider supporting digital identity assurance means for use-cases involving human representatives, and prepare SPs to support digital certificates from non-EU parties that come under different regulation than eIDAS in order to ease SCSN adoption among international participants.

# Table of contents

## **1. Introduction Case Study**

2. Key Findings Analysis
3. Proposed LoA Framework
4. High Level Roadmap for Execution
5. Research Appendix

# SCSN is a 'live' data space seeking new mechanisms to ID assurance to scale their initiative in the near future

## Description of SCSN case study

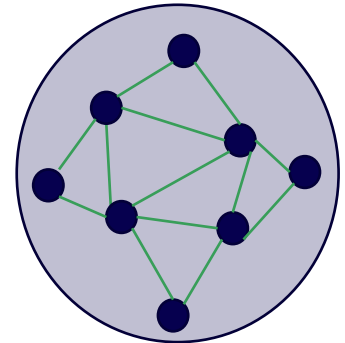


- **SCSN is a growing data sharing network** in the manufacturing sector in terms of adoption, user base variety and geography.
- When **sharing** (sensitive) **data**, **trusting** that only the intended **recipients receive data** is essential
- To **realise a high degree of assurance level for its participants** in the counterparty's digital identity, SCSN is seeking use of a digital identity assurance framework

## Relevance Case Study

Results and insight from case study are relevant to:

- **Any type of B2B 'many-to-many' data sharing** initiative in which SMEs share data
- Initiatives with **ambition to grow adoption, use cases and internationally**
- Initiatives seeking mechanisms **to increase trust** in ID of end-users **to mitigate risks** in data sharing
- Initiatives with a **wide variety of users** (a.o. corporates, start-ups)
- Initiatives that **do not have federated ID assurance** through 3rd party ID providers



Source: Data Sharing Coalition analysis

6 Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.







# SCSN case-study focused on ways to improve digital identity assurance in the B2B 'many-to-many' data sharing context

## Case study Overview

<b>Description</b>	<ul style="list-style-type: none"><li>DSC analysed the data sharing model, growth factors and needs of users of SCSN network in combination with best practices from other data sharing initiatives in terms of establishing digital identity assurance.</li></ul>
<b>Key Challenges</b>	<ul style="list-style-type: none"><li>Developing trust in data transactions between parties in the growing network, and for various levels of assurance</li><li>Dealing with increased risk due to change of scope of the network (i.e. when expanding geographical and operational scope and a user-base).</li></ul>
<b>Goal</b>	<ul style="list-style-type: none"><li>Set up appropriate identity assurance framework to stimulate adoption and mitigate risks during different growth phases of the B2B data sharing network</li></ul>
<b>Scope</b>	<ul style="list-style-type: none"><li>Improving digital identity assurance for the end-user (LoA for Service Providers is outside of the scope)</li></ul>

# SCSN's case has been developed by both SCSN, DSC participants and (at least) 5 data sharing standards have been analysed

## The following parties have been interviewed:

#	Name	Logo	Role
1	Exact		SCSN service provider
2	Tradecloud		SCSN service provider
3	Supply Drive		SCSN service provider
4	ECl Gatewise		SCSN service provider
5	Kloeckner		SCSN User
6	SBR Nexus		Data Space

## The following standards have been analysed to develop best practices:

#	Name	Logo	Sources
1	iSHARE		<a href="https://ishareworks.atlassian.net/wiki/spaces/IS/overview?homepagelid=70025239">https://ishareworks.atlassian.net/wiki/spaces/IS/overview?homepagelid=70025239</a> <a href="https://dev.ishareworks.org/index.html">https://dev.ishareworks.org/index.html</a>
2	eHerkenning		<a href="https://www.eherkenning.nl/en/levels-of-assurance">https://www.eherkenning.nl/en/levels-of-assurance</a> <a href="https://eherkenning.nl/en/applying-eherkenning">https://eherkenning.nl/en/applying-eherkenning</a>
3	IDSA		<a href="https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf">https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf</a> <a href="https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-certification-scheme-V.2.pdf">https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-certification-scheme-V.2.pdf</a> <a href="https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Infografik-English.pdf">https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Infografik-English.pdf</a>
4	SBR Nexus		<a href="https://www.sbrnexus.nl/mdmb">https://www.sbrnexus.nl/mdmb</a> <a href="https://www.sbrnexus.nl/filemanager/uploads/documenten/softwareleveranciers/201811-aansluitnotitie-softwareleveranciers.pdf">https://www.sbrnexus.nl/filemanager/uploads/documenten/softwareleveranciers/201811-aansluitnotitie-softwareleveranciers.pdf</a> <a href="https://www.sbrnexus.nl/filemanager/uploads/documenten/handleidingen/201903-handleidingPKI.pdf">https://www.sbrnexus.nl/filemanager/uploads/documenten/handleidingen/201903-handleidingPKI.pdf</a> <a href="https://www.sbrnexus.nl/filemanager/uploads/documenten/handleidingen/201811-aansluitnotitie-intermediairs.pdf">https://www.sbrnexus.nl/filemanager/uploads/documenten/handleidingen/201811-aansluitnotitie-intermediairs.pdf</a>
5	Gaia X		<a href="https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf">https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf</a> <a href="https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-Trust-Framework-22.04.pdf">https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-Trust-Framework-22.04.pdf</a>



# Most important terms used in this document


Term	Explanation
<b>Identification</b>	The process of attributing/issuing an identity to a subject by an authority. This includes issuing a digital identity after physical identity has been verified for example during an onboarding process.
<b>Authentication</b>	The process where the validity of a claimed identity is verified.
<b>Levels of Assurance (LoA) Framework</b>	A trust framework that enables many-to-many transactions through business, legal, operational, functional, and technical agreements, tools, and processes which facilitate trusted transactions between participants in a data sharing context.
<b>Identity Assurance</b>	The degree of certainty that a claim to a particular identity can be trusted to actually be the claimant's "true" identity.
<b>eIDAS Regulation</b>	The EU Regulation on electronic Identification, Authentication and Trust Services ( <a href="#">eIDAS</a> ) on electronic transactions in the EU market, established for businesses, citizens and public authorities to carry out secure electronic interactions.
<b>Digital Certificates for qualified electronic Seals under eIDAS</b>	A certificate issued to the legal and/or physical entity by a Qualified Trusted Service Provider (QTSP) for officially sealing digital documents and/or messages and is used for authenticating the entity behind the document/message.
<b>Financial Risk</b>	A risk that is incurred by a data sharing participant in case of fraud. It involves potential loss of cash and/or other liquid assets, as well as loss and damage of tangible assets like raw material, inventory and equipment.
<b>Reputational Risk</b>	A risk that is incurred by a data sharing participant which involves reputational damage to the company brand due to mis-use of digital identity or fraudulent actions during data sharing.
<b>Compliance Risk</b>	A risk that is incurred by a data sharing participant which involves exposure to legal penalties due to non-compliance to industry laws and regulations, and internal policies or clauses within contracts.
<b>Service Provider</b>	A party that carries out a range of pre-specified services to other parties in a data sharing context (e.g. verifying the identity of participants, establishing a technical connection for sending/receiving messages and data.)
<b>End-User</b>	A party that uses services in a data sharing context, could be both a sender and a receiver of data. In the SCSN context, end-user is referred to a manufacturing company that participates in data sharing within the SCSN network.
<b>Source-to-Contract (S2C)</b>	A phase in a procurement process in supply chain management where decisions regarding supplier selection are carried out. In a data sharing context parties exchange information to explore commercial deals during this phase.
<b>Procure-to-Pay (P2P)</b>	A phase in a procurement process in supply chain management where parties exchange information regarding orders and delivery.


# Table of contents


1. Introduction Case Study
- 2. Key Findings Analysis**
3. Proposed LoA Framework
4. High Level Roadmap for Execution
5. Research Appendix


# Analysis indicate that LoA framework should gradually mature through adding measures while preserving usability and adoption


## Key findings

1  Service Providers in SCSN network do not onboard and authenticate end-users in uniform fashion

2  Compliance, reputation and financial risks will increase through:  
(1) expansion of SCSN message capabilities (i.e. new use cases),  
(2) geographical network growth (e.g., Belgium, Germany)  
(3) user base and variety increase (e.g., small SMEs, corporate)

3  Identity assurance can lower associated risks. However, both SCSN's service providers and end-users demand reasonable implementation efforts

4  A one-size fits all solution for LoA is not feasible due to the diversity of technical capabilities and usability needs of SCSN user groups

5  Analysis show that other data sharing initiatives use identity assurance solutions regulated under eIDAS which allow for future scalability and trust

## Main implications

▶ A lack of uniform experience can raise concerns and frictions amongst Service providers (i.e. misaligned expectations). The network would benefit from aligning on onboarding and user experience

▶ The network is advised to increase identity assurance since adding new users and facilitating new use cases make data sharing more complex and risky

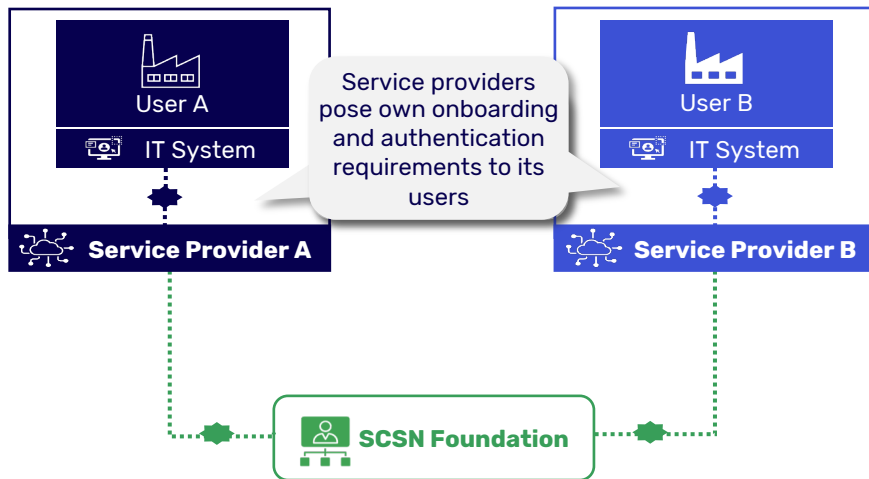
▶ The network should take measures in 3 key areas: identification, authentication and risk-mitigating policies, but balancing it with implementation hassle is key to ensure adoption

▶ LoA framework should have at least two levels of assurance (e.g., base and plus) to balance user needs, implementation efforts and trust

▶ The network with growth ambitions is advised to put eIDAS certification in it's LoA framework to support uniform onboarding experience for users, increase clarity on identity, while providing high assurance

# Friction and mis-use of identity is caused when Service Providers do not onboard and authenticate end-users in uniform fashion

## 4-corner model SCSN



### Legend:

- Trust between User and their SP is based on individual agreements
- Trust between SPs and SCSN foundation based on contractual liability agreements and issued digital certificates to SPs

## Explanation

- Data sharing in SCSN network is organised in the form of a 4 corner model where manufacturing companies (Users) exchange supply chain data with each other through their Service Providers (SPs), who establish IDS connection on behalf of their Users
- SPs are responsible for onboarding and authenticating Users to SCSN network. This procedure is not uniform amongst service providers
- Current Users' trust in the digital identity assurance in SCSN is substantiated only by liability agreements between SPs and SCSN foundation.
- SCSN issues digital certificates to SPs only, while end-users do not have digital certificates for identification and authentication purposes in the network.

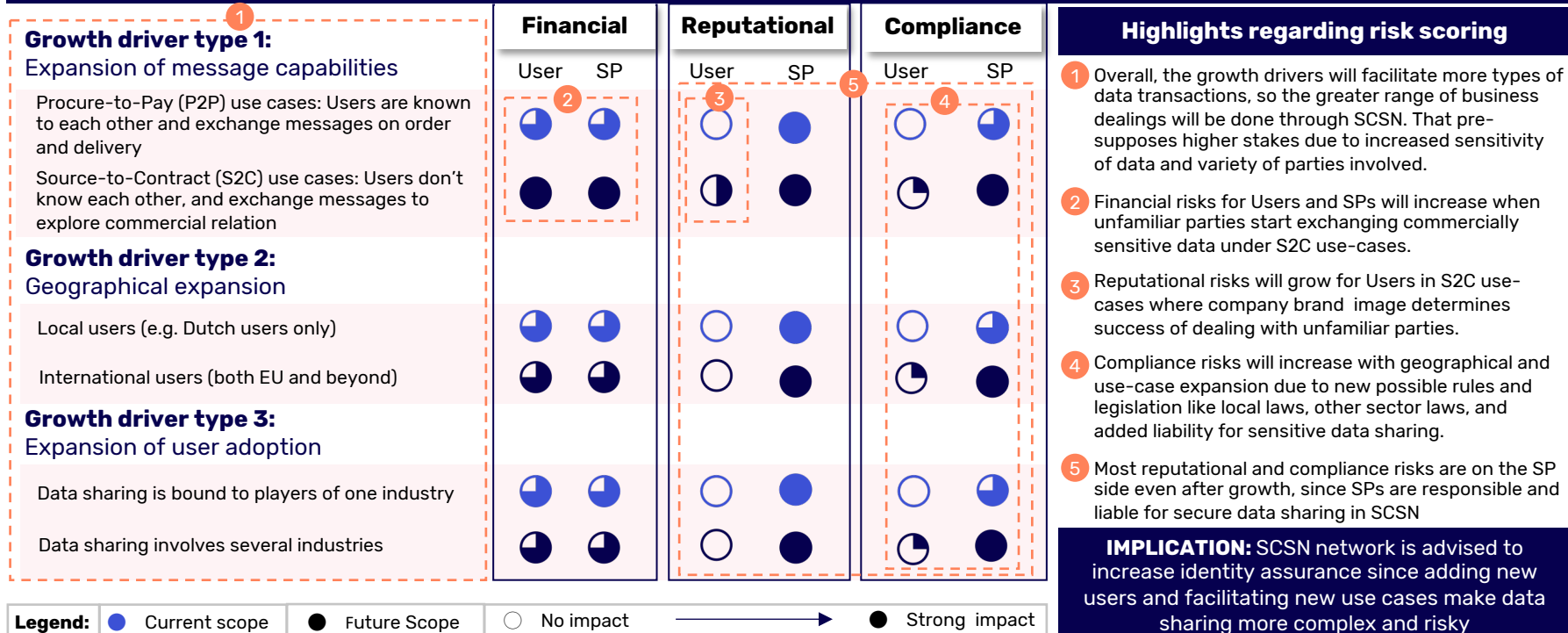
### This has resulted in:

- Implicit trust is placed on SPs with lack of instruments for them to uniformly establish assurance in the digital identity of the SCSN Users
- Some SPs show concern for reputational impact in case mis-use of digital identity occurs in the network.

**IMPLICATION:** A Lack of uniform experience for end-user's onboarding and authentication raises concerns and frictions amongst Service Providers. SCSN network would benefit from aligning requirements and expectations amongst Service Providers.

# The network's ambition to grow users base, geographical scope and functional capabilities will highly impact associated risks

## 3-fold expansion with time increases the risks of sharing data over the network (as exemplified by SCSN development)



**Legend:** Current scope Future Scope No impact Strong impact

**Source:** Data Sharing Coalition analysis

**13** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

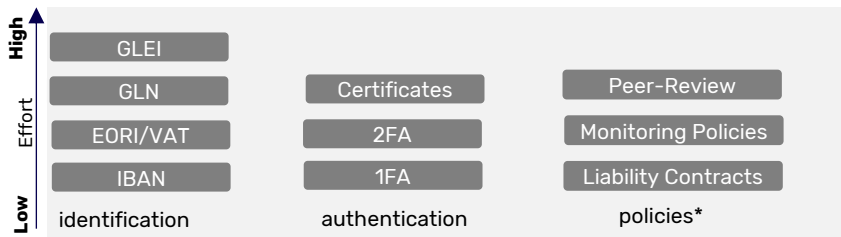
# Lowering risks with assurance solutions is about balancing trust and implementation efforts while ensuring user adoption

## End-users demand more functionality whilst ensuring trust

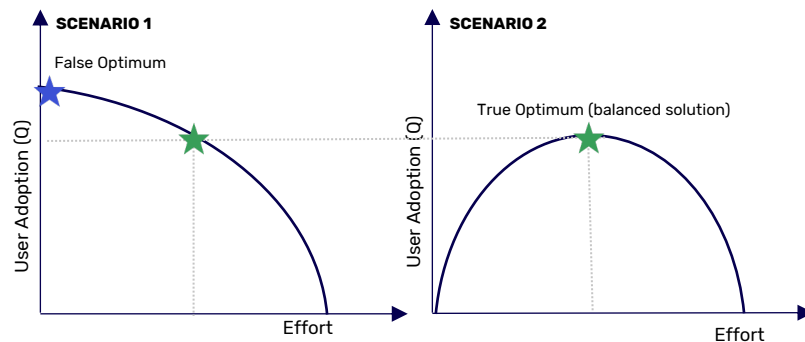
- SCSN end-users currently value low barriers to join the network and ease of use in data sharing
- For the future, SCSN's end-users are mostly interested in increasing the scope of message capabilities to facilitate more data sharing use cases
- Herein end-users acknowledge that use cases drive risks because more commercially and/or privacy-sensitive data will become part of transactions.
- More certainty on DI is key, but low implementation hassle too

## Adding trust requires substantial effort

- To increase assurance in identity, SCSN should focus on the three elements **a)** identification, **b)** authentication **and c)** risk mitigating policies
- Each underlying mechanisms comes with implementation effort. Below a visual stack of mechanisms per element, including indication of efforts
- \* Identification and authentication require direct effort from end-users, while additional policies directly impact Service Providers.



## Finding optimum between trust and effort is key



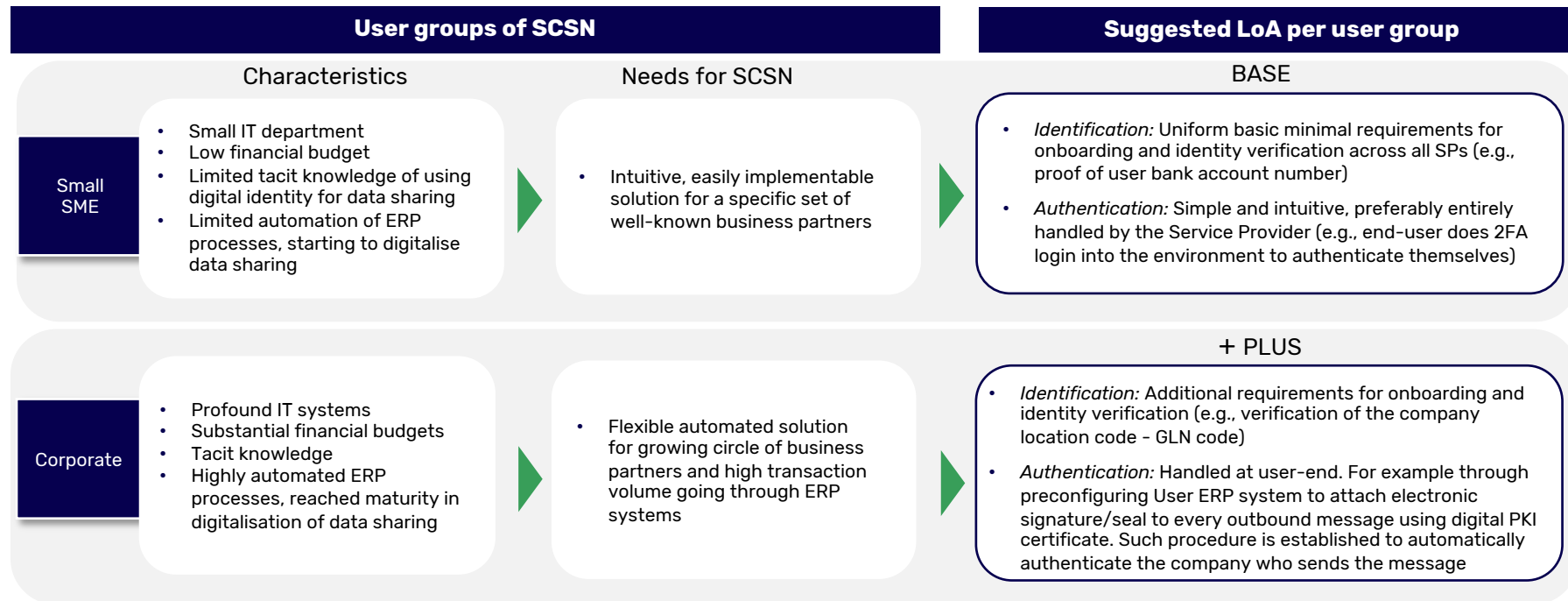
**Legend:** ★ False Optimum when risks are not accounted for    ★ True Optimum (balanced solution)

### Explanation:

- Typically user adoption drops with required implementation effort, if risks are not taken into account (see scenario 1). Thus it might seem the lowest effort solution is optimal.
- However, lower effort solutions are not efficient at addressing all risks, so risk-averse users will leave the network, lowering adoption (see scenario 2).
- Hence, the optimal solution is the one that balances risks and efforts, resulting in a highest possible adoption.

**IMPLICATION:** SCSN network should take measures in 3 key areas: identification, authentication and risk-mitigating policies but should balance it with implementation hassle to ensure adoption

# Diversity of technical abilities and needs of SCSN user groups requires two different levels of assurance in LoA framework








**IMPLICATION:** LoA of a network with distinct user groups should have at least two levels of assurance (base and plus) to balance user needs, implementation efforts and trust

# eIDAS based digital ID solutions, as used in other sectors, can simplify onboarding for users and provide high assurance

## Digital Identity assurance in other data sharing initiatives

The table below summarises the use of digital certificates for establishing higher identity assurance in other large-scale data sharing initiatives compared to SCSN network

Initiative	User Type	LoA Issuer	Assurance means
 iSHARE	Legal entity and natural person	Qualified Trusted Service Providers (QTSPs) issuing certificates under eIDAS regulation	X.509 digital certificates for eIDAS QESeals are used by parties to obtain access tokens for authentication and data sharing
 SBR NEXUS	Legal entity and natural person		X.509 PKI-Overheid certificates under eIDAS are used by parties to obtain access tokens to authenticate and exchange messages (for human representatives eHerkenning login means are used)
 gaia-x	Legal entity		W3C verifiable credentials with cryptographic signatures, among which eIDAS digital certificates for eSignatures are used to authenticate parties.
 ID SA	Legal entity	Certification Authority (CA) established within IDSA	X.509 digital certificates are used to authenticate Users and obtain access tokens for sharing data
 SCSN smart connected supplier network	Legal entity	SCSN Foundation	Login means for end-users to identify and authenticate themselves at their Service Provider; there is no end-user PKI certification

## Explanation

- Analysis show authentication means regulated under eIDAS are becoming a standard implementation in other data sharing initiatives
- eIDAS regulated means provide scalability of trust because the role of verifying digital identity of Users is federated and outsourced to qualified 3rd parties.
- Overall, digital certificates for eIDAS QESeals and/or eSignatures, as used by other data sharing initiatives, aid in authentication of legal entities (parties) and protect integrity of digital claims as they bind the message to the identity of the certificate's owner

**eIDAS can bring the following value to data sharing networks that do not yet rely on it:**

- 1. Higher assurance** because: (a) a user is signing (sealing) each of their messages/requests, (b) certificates are issued by qualified trusted parties that thoroughly verify User identity.
- 2. Simplified onboarding:** prior or obtaining the certificate User is verified by a trusted party, hence there are less checks for SP to conduct
- 3. Low implementation effort by SPs** as the eIDAS means will become common and required by regulation, and will be interoperable across EU.

**IMPLICATION:** To identify and authenticate end-users it is advised to implement eIDAS certification in the LoA framework. Such solution can better support uniform onboarding experience for users, increase clarity on identity, while providing high assurance

Source: Data Sharing Coalition analysis

16 Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.



# Table of contents

1. Introduction Case Study
2. Key Findings Analysis
- 3. Proposed LoA Framework**
4. High Level Roadmap for Execution
5. Research Appendix

# To achieve improved LoA framework, solutions with 2 assurance levels (plus and base) and additional policies need to be set up

## Blueprint to decide for which use-cases which LoA level is suitable

- In a growing B2B data sharing network like SCSN 3 possible use-cases are identified (rf. table below):
  - end-users know each other prior to engaging in machine-to-machine (M2M) data sharing
  - end-users do not know each other prior to engaging in M2M data sharing
  - Human representatives are involved in data sharing
- Use-cases differ in terms of growth drivers and main risks for the User, which determines which level of assurance is recommended for that use-case:

#	Use-case Description	Growth Drivers			Main risks for a User	Recommended LoA	
		Messages scope	Geo scope	Adoption size		I&A Level*	Other Policies
1	M2M (data sharing between ERP systems)	P2P data transactions	Local	Parties operate in the same sector	Financial risk if any assets are lost due to fraud	Base	
2	M2M (data sharing between ERP systems)	S2C data transactions	International	Cross-sectoral data sharing	In addition to financial, compliance risk occurs due to added local regulations	Plus	Liability Contracts Peer Review Monitoring Policies
3	H2M (human representative is involved)	Full procurement	International	Cross-sectoral data sharing	Financial if sensitive data reaches malicious party	Plus with extra considerations for H2M	

**Abbreviations:** I&A stands for identification and authentication procedures, P2P – Procure-to-Pay, S2C – Source-to-Contract, M2M – machine-to-machine, H2M – human-to-machine

**Source:** Data Sharing Coalition analysis

**18** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# Base Level assurance consists of identification and authentication measures that satisfy less tech-savvy user group

## Base Level Assurance means and their implementation in SCSN

- Base level consists of two procedures - identification and authentication of digital identity of a User that have low to medium implementation efforts.
- Table below summarises elements and processes for the the two procedures and lists reasons for their implementation.

Element	Verification Process	Reasons to verify	Effort for Implementation	
<b>Base Level Identification</b>			<b>For User</b>	<b>For SP</b>
<b>Contact email address</b>	User provides an email address and follows a link in the SP's email request to prove the email ownership	To have correct contact for future correspondence and updates	Low	Low
<b>Chamber of commerce registration</b>	User provides the official extract document from chamber of commerce with EORI/VAT* number	EORI/VAT and IBAN checks together are needed to verify that official registered company matches the details of the used bank account to reduce fraud	Medium	Low
<b>Corporate bank account details</b>	Administration department of a User sends 1 € direct debit payment to SP's bank account		Medium	Low
<b>Physical location of a business</b>	User obtains GLN code under the GS1 standard (SP personally buys and supplies GLN to a User)	Checking GLN ensures that correct physical end-point will receive SCSN messages	Low	Medium
<b>Base Level Authentication</b>				
<b>Two Factor Authentication (2FA)</b>	User logs in with a username-password combination and a PIN-code from a physical device (e.g. mobile-app, SMS, USB-stick)	Provides higher assurance since likelihood of a hack is significantly reduced	Low	Low (for SPs who already use 2FA)

### Conclusion/remarks about Base level:

- The network's authority is advised to discuss together with all Service Providers on how specific procedures need to be set up.
- EORI and VAT number are both used as an ID of a legal entity across the EU, while VAT is used by non-EU countries. SPs with network authority can decide preferred option.
- SPs can provide GLN code to the Base level Users to avoid hassle, however with time users should buy GLN on their own to strengthen assurance and avoid security issues.

# Plus Level assurance consists of identification and authentication measures that satisfy users with advanced needs

## Plus Level Assurance means and their implementation in SCSN

- Plus level consists of two procedures - identification and authentication of digital identity of a User that have medium to high implementation efforts, but mitigate risks to better extent compared to the Base level assurance

Element	Verification Process	Reasons to verify	Effort for Implementation	
<b>Plus Level Identification</b>			<b>For User</b>	<b>For SP</b>
<b>Contact email address</b>	User provides an email address and follows a link in the SP's email request to prove the email ownership	To have correct contact for future correspondence and updates	Low	Low
<b>Chamber of commerce registration</b>	User provides the official extract document from chamber of commerce with EORI/VAT* number	EORI/VAT and IBAN checks together are needed to verify that official registered company matches the details of the used bank account to reduce fraud	Medium	Low
<b>Corporate bank account details</b>	Administration department of a User sends 1 € direct debit payment to SP's bank account		Medium	Low
<b>Physical location of a business</b>	User provides GLN code under the GS1 standard User buys GLN independently of SP for SP to verify it	Checking GLN ensures that correct physical end-point will receive SCSN messages	Medium	Low
<b>Plus Level Authentication</b>				
<b>eIDAS Digital Certificate for electronic seal/signature</b>	User follows procedures of a QTSP under eIDAS to purchase and obtain the certificate	Public and private keys in a digital certificate are needed to authenticate a User of the message	High	Medium
<b>eHekening login means</b>	Purchased from a QTSP under eIDAS	Needed to authenticate a human representative	High	Low

### Conclusion/remarks about Plus level:

- The network authority is advised to discuss together with all Service Providers on how specific procedures need to be set up.
- Given that different digital certificates for identifying businesses exist under eIDAS (certificates for eSeals/eSignatures), it is up to the network authority and SPs to choose.
- eIDAS certificates will add transparency in the network, since sender can sign/seal a message as a proof of their identity for receiver to see. This is a user-to-user solution.
- eHekening login means for human representatives are given as an example measure for H2M use-cases, since this is a Dutch implementation.

Source: Data Sharing Coalition analysis

20 Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# Peer reviews, monitoring policies and liability contracts should be part of the additional risk-mitigating measures to improve trust

## Other risk-mitigating policies and their implementation in SCSN

- Risk mitigating policies (measures) require effort from SPs and SCSN to set up and follow.
- They consist of solutions that act as preventative mechanisms to ensure higher level of assurance in the B2B data sharing network.

Element	Description of Procedures	Reasons to implement	Effort for Implementation	
			For User	For SP
<b>Liability Contracts</b>	<ul style="list-style-type: none"> <li>• A list of Standard Clauses to be signed by parties prior to joining/using/providing services in SCSN</li> </ul>	Needed to ensure that SPs identify and authenticate Users responsibly	Low	Low
<b>Peer Review Process for SPs</b>	<ul style="list-style-type: none"> <li>• Workshops, reflective touchpoints, surveys/interviews and means to share and analyse input from SPs and Users regarding improvements of SCSN LoA framework</li> </ul>	Needed to (1) align views and interests of SPs on a current state of onboarding procedures and (2) identify common agreed upon solutions.	Low	Medium
<b>Monitoring policies</b>	<ul style="list-style-type: none"> <li>• Warnings and checks when vital User identity data has been changed</li> <li>• Process policies to handle data requests with insufficient assurance level</li> </ul>	Needed to create mechanisms for detecting mis-use of digital identity and preventing fraud	Low	Medium

## Conclusion/remarks about additional policies:

- The network authority is advised to discuss together with all Service Providers on how specific procedures need to be set up.
- Additional policies are meant to aid Service Providers and hence should be established after mutual common agreement.

# Table of contents

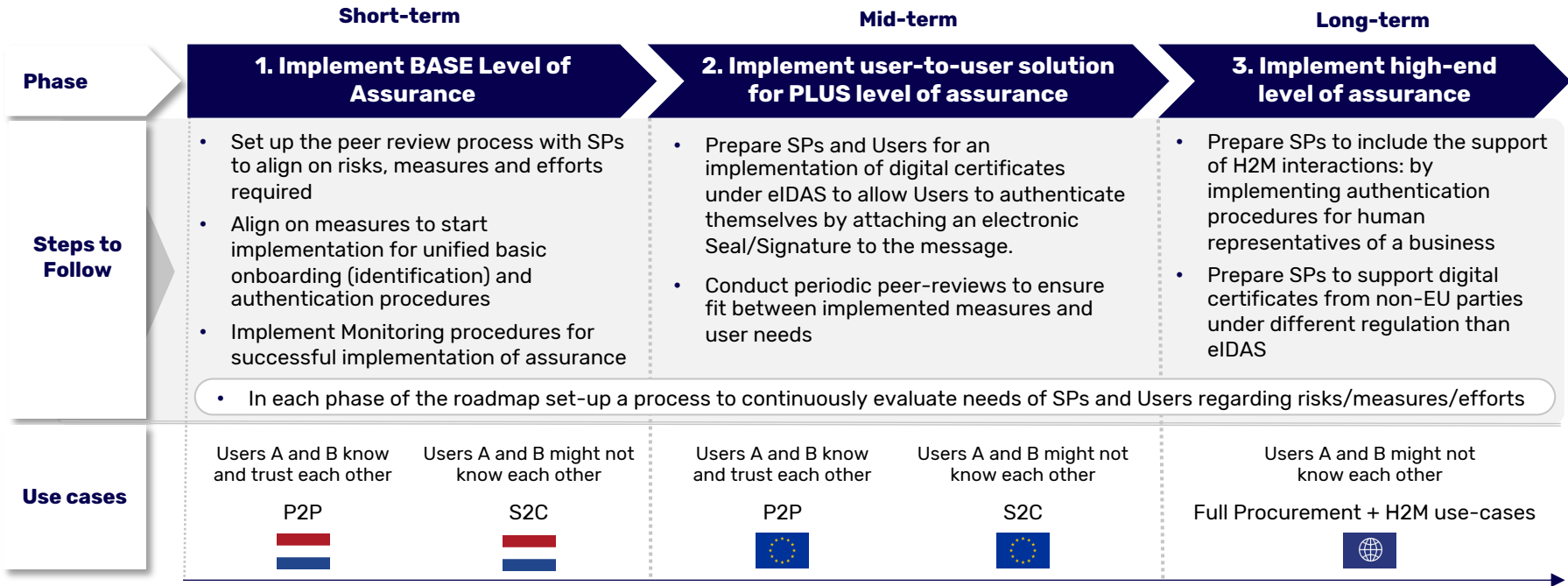
1. Introduction Case Study
2. Key Findings Analysis
3. Proposed LoA Framework

## 4. High Level Roadmap for Execution

5. Research Appendix

# Roadmap provides concrete steps to implement LoA framework and manage risks associated with increasing the scope

## Roadmap for improving digital identity assurance framework using the SCSN case-study as an example



**Abbreviations:** SP – service provider, P2P – Procure-to-Pay, S2C – Source-to-Contract, H2M – human-to-machine.

**Source:** Data Sharing Coalition analysis

**23** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# Table of contents

1. Introduction Case Study
2. Key Findings Analysis
3. Proposed LoA Framework
4. High Level Roadmap for Execution

## **5. Research Appendix:**

- Background information on SCSN network
- Interviews with SCSN network participants
- Research on assurance in data sharing initiatives (iShare, SBR Nexus, Gaia-X, IDSA)
- Research on assurance means regulated under eIDAS (eHerkenning, PKI-Overheid, QESeals)



# Table of contents

1. Introduction Case Study
2. Key Findings Analysis
3. Proposed LoA Framework
4. High Level Roadmap for Execution

## **5. Research Appendix:**

- Background information on SCSN network
- Interviews with SCSN network participants
- Research on assurance in data sharing initiatives (iShare, SBR Nexus, Gaia-X, IDSA)
- Research on assurance means regulated under eIDAS (eHerkenning, PKI-Overheid, QESeals)

# SCSN enables scalable data sharing for manufacturing industry by solving key data sharing challenges

## Key data sharing challenges in manufacturing supply chain



**Traditional connections** between manufacturing companies **are set up bilaterally**. Each additional company requires a new connection which serves as a **scalability barrier**



**Using platforms** to connect manufacturing companies leads to data **monopolies and fragmentation** between the different platforms



**The lack of trust** hinders **data sovereignty** of the manufacturing companies. Thus, making it hard for them to share data and to remain in control over **sensitive data**

## Solution offered by SCSN

SCSN is a data standard that makes sharing information within supplier networks more efficiently. The data standard allows for quicker, easier and more controlled data exchanges.

## Participants (non-exhaustive)

### Service Providers (7)



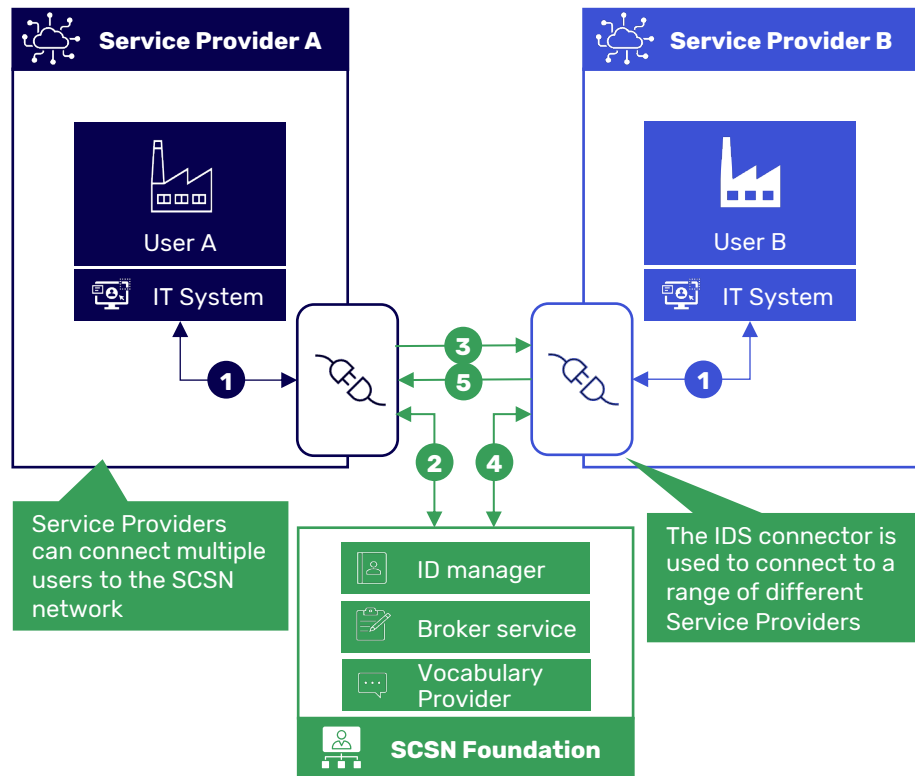
### Connectors (10)



### Manufacturing companies (300+)



# In SCSN manufacturing companies (Users) exchange supply chain data by connecting to one of the Service Providers



Step:	Description:
1	User A and User B join the SCSN network by connecting to Service Providers A and B respectively
2	User A requests the ID manager and Broker Service via Service Provider A's IDS Connector to provide validated credentials from Party B
3	User A composes a data request message using the data standard defined by the Vocabulary Provider and sends it to Party B via Service Provider A and Service Provider B
4	User B requests the ID manager and Broker Service Service Provider B's IDS Connector to validate the credentials from party A
5	User B composes a data response message using the data standard defined by the Vocabulary Provider and sends it to Party A via Service Provider B and Service Provider A









## Legend

- IDS connector from corresponding Service Provider
- Custom language (IT System and Service Provider dependent)
- Interaction in SCSN language according to IDS standards

**Source:** Data Sharing Coalition analysis based on <https://smart-connected-supplier-network.gitbook.io/>

**27** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# Detailed description of roles and functionalities in interaction model of SCSN network

	Icon	Name	Description
<b>Roles</b>		Manufacturing company	Original equipment manufacturers, manufacturing companies, suppliers, or other companies in supply chains participating in SCSN to share data with others in the supply chain
		Service providers	IT partners who facilitate the connection to the SCSN network for companies in the manufacturing industry
		IT system providers	Providers of software used by organisations to manage daily business activities
		Smart Connected Supplier Foundation	Foundation currently managing and expanding the network, providing support, developing additional messages, and making the network more professional
<b>Functionalities</b>		Identity Manager	Management of identities (certificates) of service providers. For each data exchange, certificates are checked for authenticity and validity
		Broker service	Overview of parties affiliated with SCSN. The address book contains the following for each company: organisation name, unique ID, supported messages, connected service provider
		Vocabulary Provider	The Vocabulary Provider defines the type of messages on the SCSN network and the data format used within the messages
		IDS Connector	The IDS Connector is the technical component for data exchange of the SCSN Vocabulary between manufacturing companies and service providers. Service providers use temporary tunnels to communicate data.

**Source:** Data Sharing Coalition analysis based on <https://smart-connected-supplier-network.gitbook.io/>

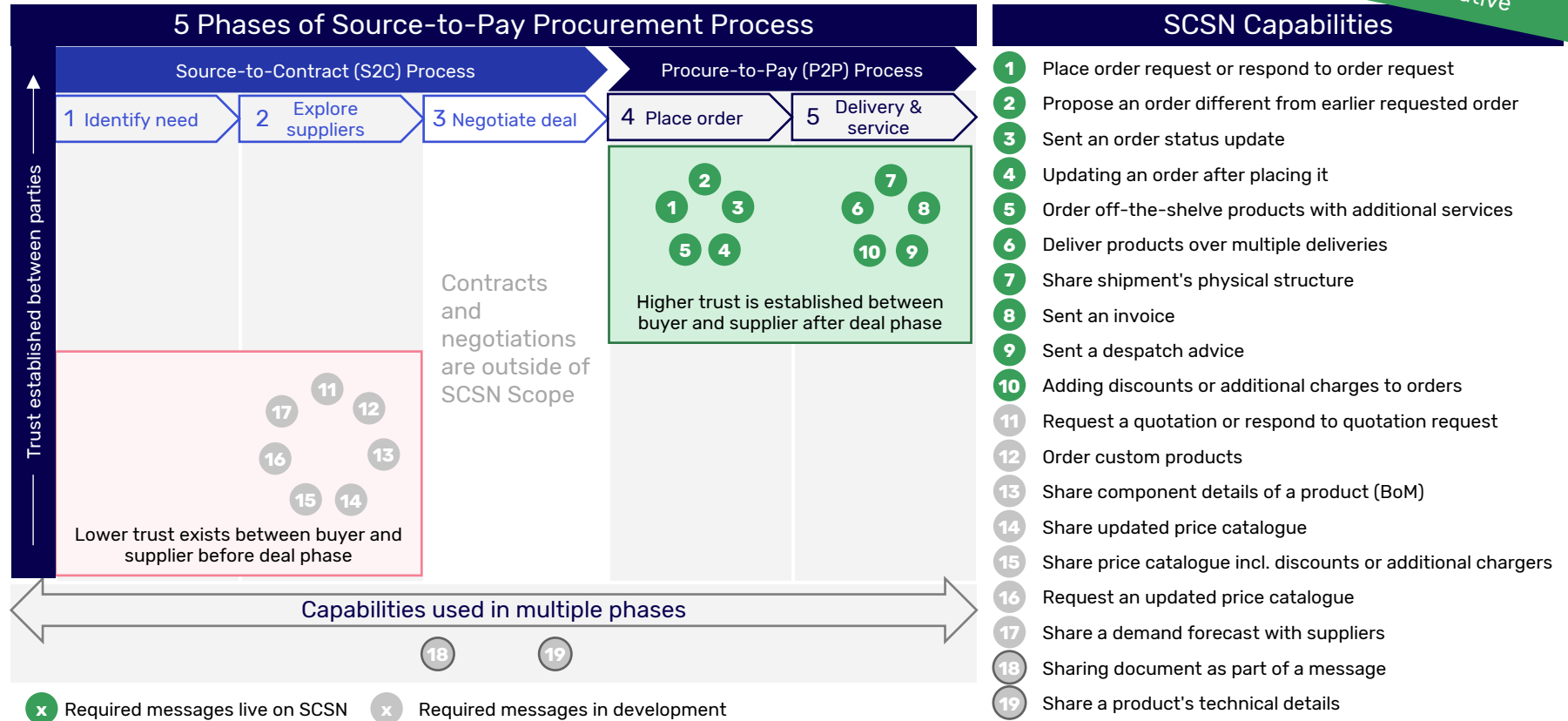
**28** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# SCSN Admission criteria are focussed on technical compliance according to Gitbook and other shared info



Introduction to SCSN		Key observations from current LoA framework	
<ul style="list-style-type: none"> <li>The goal of the Smart Connected Supplier Network (SCSN) is enabling the manufacturing industry to share data across company borders in an easier, safer, and more reliable way</li> <li>SCSN developed a communication standard to be used in a four corner model, where manufacturing companies share data via service providers to enhance scalability and prevent data monopolies by platforms</li> </ul>		<p>Information on Gitbook regarding issuance of assurance levels to end-users is limited</p> <p>Trust in the network is assured through liability contracts between Service Providers and SCSN foundation</p>	
LoA Framework X	<b>General characteristics</b>	<b>Identity owner</b> <input type="checkbox"/> Natural person <input checked="" type="checkbox"/> Legal person <b>Liability agreements for mis-use of ID</b> <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<b>LoA Issuer</b> <input type="checkbox"/> Scheme Authority <input checked="" type="checkbox"/> Certified participants <input type="checkbox"/> Other <b>LoA is shared in the network by</b> <input type="checkbox"/> no specific means besides liability contracts
	<b>LoAs used</b>	<b>Typical u/cs per LoA</b>	<b>Most relevant risks in u/c</b>
	Participant (User) level	<ul style="list-style-type: none"> <li>Manufacturing company A requests/sends data to manufacturing company B via their Service Providers A and B respectively, who establish IDS connection for sharing data</li> </ul>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 2px; display: inline-block;">Financial</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px; display: inline-block;">Reputational</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">Compliance</div>
		<b>LoA criteria</b>	
		<ol style="list-style-type: none"> <li>Deployed IDS Connector, registered in the SCSN data space</li> <li>General organisation information</li> <li>Integration of the organization's back-end system and the OpenAPI Data App</li> </ol>	

# Currently live SCSN capabilities are clustered in the latest phases of procurement processes



Source: Data Sharing Coalition analysis

# The SCSN data space is composed of nine building blocks that together realise trusted data sharing

SCSN trust components are assessed through the nine building block model

## Business model

- Service Providers are free to choose a business model towards their customers (i.e. there are no restrictions from SCSN)
- Service Providers are paying fees to the SCSN foundation based on the number of connected companies

## Governance

Roles in the network consist of the Board, Supervisory Board, Service Providers and Manufacturing companies. Network governance is facilitated by the Board and Supervisory board.

## Legal agreements

There is no public information on legal agreements between the Foundation and Service Providers or between the Foundation and users. There are no data space level requirements on legal agreements between Users and Service Providers

## Operational agreements

End user-support is provided to Service Providers by the SCSN foundation. Working groups are in place where participants can contribute to developments and shape future of the SCSN Foundation.

## Metadata

SCSN's metadata agreements are based on the IDS standard for the structure and semantics of metadata of data that is being shared throughout the network.

## Security

Service Providers are responsible for the security of a connector. The IDS connectors are IDSA approved, and thereby meeting the standards for security and functionality

## Identification, Authentication and Authorisation (IAA)

- Global Location Numbers are used as identifiers
- Authentication and Authorisation is technically implemented using IDS connectors
- Admission criteria on data space level are covering technical requirements, service providers can impose their own requirements

## Exchange protocol

International Data Spaces (IDS) is the technology under SCSN's four-corner model. IDS provides a secure and sovereign data exchange among trusted partners.

## Data standards

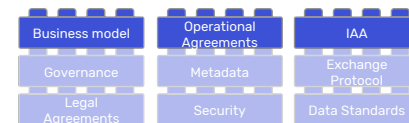
The SCSN data standard is based on Universal Business Language (UBL) and the European Norm for e-invoicing. It defines a common language for how supply chain information is shared.




In-depth description of design choices for all building blocks is available on next pages

**Source:** Data Sharing Coalition based on <https://smart-connected-supplier-network.gitbook.io/>

**31** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# Detailed explanation of the nine building block model which covers the soft infrastructure layer (1/3)



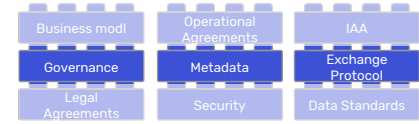
Building block	 <b>Business model</b>	 <b>Operational agreements</b>	 <b>Identification, authentication, and authorisation</b>
Description	Specification of the business model of data sharing for actors in the use case	Common agreements on relevant operational procedures	Common practices and tools for identification and authentication of actors and the way actors deal with authorisation of data access
Underlying topics (non-exhaustive)	<ul style="list-style-type: none"> <li>Services and value propositions in use case</li> <li>Compensation mechanisms between actors in use case</li> </ul>	<ul style="list-style-type: none"> <li>SLAs</li> <li>End user support</li> <li>Audit trails and archiving</li> </ul>	<ul style="list-style-type: none"> <li>Identifiers used for actors</li> <li>Method of identification</li> <li>Authentication requirements</li> <li>Levels of Assurance</li> <li>Authorisation flow and requirements</li> <li>Authorisation management</li> </ul>
In scope of SCSN	Service Providers can use their own <a href="#">business model</a> for connecting manufacturing companies and processing messages.	SCSN provides end-user support in the form of developer tools such as an <a href="#">XML eValidation</a> service and a <a href="#">community portal</a> . SCSN does not provide implementation <a href="#">support</a> .	<p>Each organisation connected to SCSN is uniquely identifiable using a Global Location Number. SP admission requirements (<a href="#">source</a> see <a href="#">also</a>):</p> <ul style="list-style-type: none"> <li>Deployed IDS connector registered in SCSN data space, general organisation information, integration of organisation's back-end system and OpenAPI Data App</li> <li>Location Number (existent GLN's accepted)</li> <li>Add organisation to IDS connector of SP</li> </ul>




**Source:** Data Sharing Coalition based on <https://smart-connected-supplier-network.gitbook.io/>

**32** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.



# Detailed explanation of the nine building block model which covers the soft infrastructure layer (2/3)

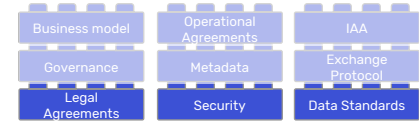





Building block	 Governance	 Metadata	 Exchange protocol
Description	Common governance structure that oversees operations, change management, disputes, etc.	Standards for the structure and semantics of metadata of data that is being shared through domain	Standards for how data is shared
Underlying topics (non-exhaustive)	<ul style="list-style-type: none"> <li>Governing bodies that oversee (transaction) activity</li> <li>Roles that require registration by an authority</li> <li>Roles that require certification by an authority</li> </ul>	<ul style="list-style-type: none"> <li>Standards used for metadata</li> <li>Metadata included in data transaction</li> </ul>	<ul style="list-style-type: none"> <li>Messaging standards</li> <li>Predefined messages</li> <li>Mapping between different data formats</li> <li>H2M communication protocol</li> <li>M2M communication protocol</li> </ul>
In scope of SCSN	<ol style="list-style-type: none"> <li>The Board: manage foundation, define long-term (LT) ambitions, approve standard changes, coordinate and implement daily activities, directing support organisation, forming and chairing working groups</li> <li>Supervisory Board: approves LT ambitions, supervising management of foundation</li> <li>Service providers</li> <li>Manufacturing companies</li> </ol>	<ul style="list-style-type: none"> <li>Based on <a href="#">International Data Spaces (IDS)</a></li> </ul>	In SCSN's four-corner model, data being shared between company A and company B is exchanged via service provider A and service provider B. Note that there is (centralised platform in between, the foundation has no role in the actual exchange of data.

**Source:** Data Sharing Coalition based on <https://smart-connected-supplier-network.gitbook.io/>

**33** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# Detailed explanation of the nine building block model which covers the soft infrastructure layer (3/3)



Building block	 <b>Legal agreements</b>	 <b>Security</b>	 <b>Data standards</b>
Description	Common agreements on all relevant legal matters such as liability, penalties, contracts, etc.	Common practices and agreements on security measures in use case	Standards for (storage of) the data that is being shared: data structure, semantics, etc.
Underlying topics (non-exhaustive)	<ul style="list-style-type: none"> <li>• Contracts and terms &amp; conditions</li> <li>• Liabilities</li> <li>• Privacy policies</li> <li>• Relevant regulation impacting use case</li> </ul>	<ul style="list-style-type: none"> <li>• Security for data in rest</li> <li>• Security for data in transit</li> </ul>	<ul style="list-style-type: none"> <li>• Architecture</li> <li>• Requirements for data storage</li> <li>• Standards for data structure</li> <li>• Taxonomies and ontologies</li> <li>• Data quality standards and measures</li> </ul>
In scope of SCSN	Not applicable as no legal agreements are required to join the SCSN network. Most legal agreements occur between manufacturing companies and service providers.	<ul style="list-style-type: none"> <li>• No additional <a href="#">security</a> measures besides the <a href="#">IDS standard</a>. Service Providers are responsible for security of their connectors.</li> <li>• GAIA-X Hub NL is looking into auditing the IDS connectors used by Service Providers in SCSN which would increase security.</li> </ul>	To facilitate communication between MCs by means of SPs and connectors, SCSN has <a href="#">predefined a universal language of message specifications</a> ; pertaining to order, despatch advice, technical product data, bill of materials, forecasting, what if, quotation, measurement, catalogue messages. <a href="#">Codes</a> are also defined.

**Source:** Data Sharing Coalition based on <https://smart-connected-supplier-network.gitbook.io/>

**34** Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.

# Table of contents

1. Introduction Case Study
2. Key Findings Analysis
3. Proposed LoA Framework
4. High Level Roadmap for Execution
- 5. Research Appendix:**
  - Background information on SCSN network
  - Interviews with SCSN network participants
  - Research on assurance in data sharing initiatives (iShare, SBR Nexus, Gaia-X, IDSA)
  - Research on assurance means regulated under eIDAS (eHerkenning, PKI-Overheid, QESeals)

# In scope of the LoA research for SCSN, interviews with four service providers and one user were carried out



## Overview of the SCSN Interview process

#	Role	Company description	Key Learnings per interview
1	Service Provider	Cloud provider connecting 10 Users to SCSN; international player but within SCSN focuses on supporting Dutch connections only.	<ul style="list-style-type: none"> <li>The <b>current scope of SCSN data space is data sharing between parties that trust each other already</b> (outside of the data space)</li> <li>'Zorgplicht' in contracts of Service Providers (SP) and SCSN Foundation puts liability for misbehaving</li> <li><b>Any stricter trust measures hinder adoption</b>, which is according to this interview the main focus for SCSN</li> </ul>
2	Service Provider	Cloud and software provider supporting 42 Users with SCSN connection, has international focus.	<ul style="list-style-type: none"> <li>Users make agreements before SCSN interactions occur, hence parties know and trust each other when sharing data on SCSN</li> <li>In the future, <b>this might change when expanding to more users/use cases</b>, where it is key to cater both SMEs and multinationals in trust requirements</li> </ul>
3	Service Provider	Cloud solutions provider supporting 14 SCSN Users but currently remains in a pilot phase, has international focus.	<ul style="list-style-type: none"> <li>The lack of SCSN wide agreements on onboarding has raised attention of internal stakeholders. <b>This group fears reputational damage, which might hinder the go live of the SP with SCSN messages</b></li> </ul>
4	Service Provider	Software provider connecting 34 Users to SCSN, mainly focused on local Dutch connections	<ul style="list-style-type: none"> <li>When improving trust, any additional measures should be <b>as easy as sending email</b> (the substitute for users), and trust requirements from both big and small organisations should be considered</li> </ul>
5	User	Prominent user and one of the ambassadors of SCSN	<ul style="list-style-type: none"> <li>This user <b> vets any user they do business with</b> (or interact with on SCSN), making the risk of interacting with unknown users minimal in current set-up</li> </ul>

### Key characteristics of SCSN LoA framework according to interviews:

- 1 Any additional measures should have minor impact on users to maintain pace of adoption
- 2 Current main risk related to lack of assurance is (indirect) reputational risk from ID mis-use (e.g. bad PR). While (direct) risks related to content of data being accessed by unauthorised parties remains limited given the current state of the network.
- 3 Additional LoA measures are required when expanding SCSN to other use cases

# Table of contents

1. Introduction Case Study
2. Key Findings Analysis
3. Proposed LoA Framework
4. High Level Roadmap for Execution
- 5. Research Appendix:**
  - Background information on SCSN network
  - Interviews with SCSN network participants
  - Research on assurance in data sharing initiatives (iShare, SBR Nexus, Gaia-X, IDSA)
  - Research on assurance means regulated under eIDAS (eHerkenning, PKI-Overheid, QESeals)

# SCSN's use cases resemble the iSHARE use cases, however iSHARE's use of QESeals significantly increases LoA



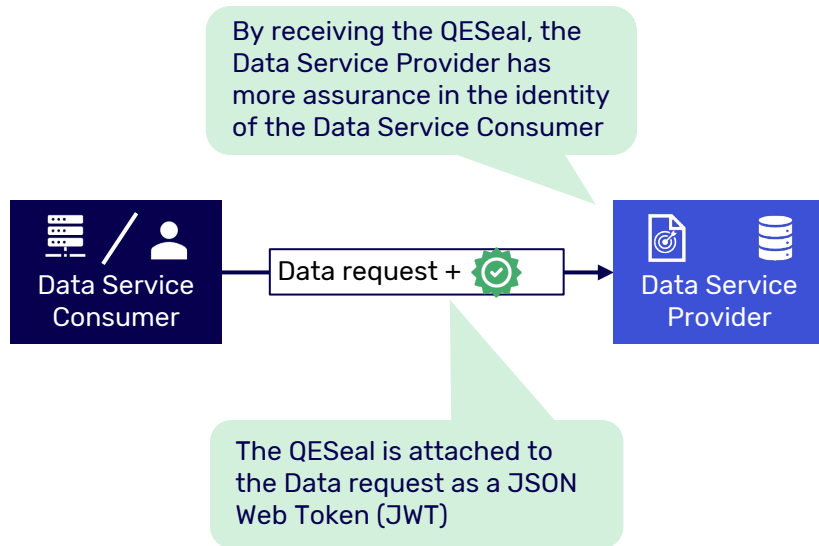
Introduction to iSHARE		Key learnings from iSHARE for SCSN on LoAs			
<ul style="list-style-type: none"> <li>The iSHARE Foundation is a non-profit organisation that aims to enable trust between parties in a network (within a specific sector, for example logistics)</li> <li>To realise this, iSHARE facilitates data sharing by offering a generic set of agreements for identification, authentication and authorisation</li> </ul>		<ul style="list-style-type: none"> <li>iSHARE M2M use cases resemble those at SCSN. Hence, it is insightful to look into additional LoA requirements that are not yet introduced in SCSN, but are present in iSHARE.</li> <li>Compared to SCSN, iSHARE uses Qualified Electronic Seals for authentication which provide a high assurance level as the use of QESeals is regulated in eIDAS</li> </ul>			
LoA Framework iSHARE	<b>General characteristics</b>	<b>Identity owner</b> Natural person Legal person	<b>LoA Issuer</b> Scheme Authority Certified participants Other		
		<b>Liability agreements for mis-use of ID<sup>1</sup></b> Yes No	<b>LoA is shared in the network by</b> use of Qualified Electronic Seal		
	<b>LoAs used</b>	<b>Typical u/cs per LoA</b>	<b>U/c Risks</b>	<b>Identification</b>	<b>Authentication</b>
Machine-2-Machine (M2M)	The ERP system (machine) of Party A requests a status update from the ERP system (machine) of Party B. Party B's ERP system automatically responds with the requested status update. No humans are needed to interfere.	Financial Reputational Compliance	<ol style="list-style-type: none"> <li>Valid EORI number</li> <li>Qualified Electronic Seal (QESeal)</li> <li>Signed iSHARE Accession Agreement</li> <li>Successful test report of iSHARE certification tool</li> <li>(Certified parties need additional criteria)</li> </ol>	See next slides QESeal is used to obtain JSON access tokens via OAuth 2.0 Protocol	
Human-2-Machine (H2M)	Human X, representing Party A, requests a status update from the ERP system (machine) of Party B. It does so via a user interface.	Financial Reputational Compliance	<ol style="list-style-type: none"> <li>M2M criteria apply</li> <li>Digital identity for natural person is issued by iSHARE-certified Identity Providers (IDPs):               <ul style="list-style-type: none"> <li>eIDAS IDPs (eHerkenning)</li> <li>SecureLogistics</li> </ul> </li> </ol>	QESeal is used to obtain JSON access tokens for human representatives via OpenID Connect 1.0 Protocol	


1. iShare Scheme Owner does not bear liability for the misconduct of the parties. All Certified Parties must safeguard the security.

Source: Data Sharing Coalition analysis based on [iShare Trust Framework v1.10](#)

# The Qualified Electronic Seal is used by the Data Service Consumer to prove it's identity to the Data Service Provider

## Visualisation of QESeals use in iSHARE



 = Qualified Electronic Seal (QESeal)

## Description of use of QESeals in iSHARE

### The WHY of QESeals:

- The overall role of QESeals is to aid in authentication of legal entities (parties) and to ensure protection of integrity of digital claims.
- Qualified Digital Certificates for electronic Seals, by following stricter requirements in the eIDAS Regulation, provide higher guarantees regarding the identity of the creator of the seal and therefore higher legal certainty.

### The WHAT of QESeals:

- QESeal binds the content of a message (in this case the data request) to the owner of a Digital Certificate, which is issued by Trusted Service Providers under the EU eIDAS Regulation.
- Electronic Seals are legally equivalent to analogue Seals (i.e. seals used on regular mail and documents).

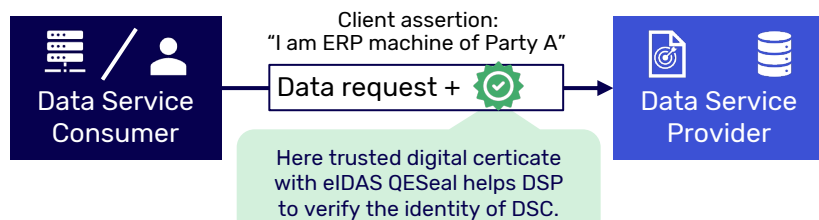
### The HOW of QESeals:

- Within iSHARE, digital certificates with QESeals are used by parties to obtain access tokens (JWT) for authentication purposes.




See next slide

# Details on How the Qualified Electronic Seal is used by the Data Service Consumer to prove it's identity

## Visualisation of QESeals use in iSHARE:

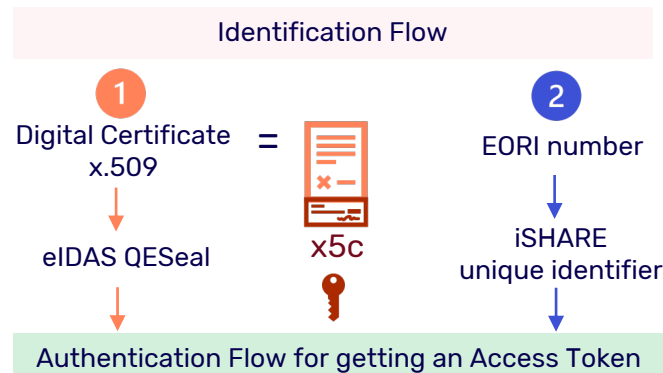


## Legend for Identification and Authentication flows:

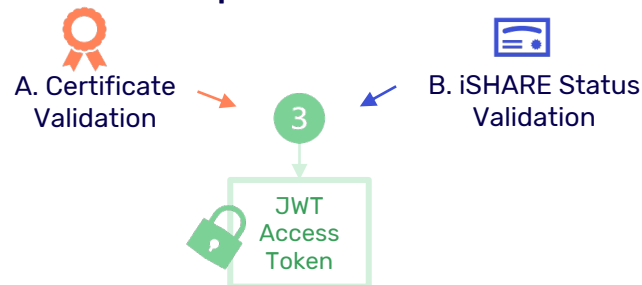
- 1 Parties need to acquire a trusted eIDAS x.509 certificate for QESeal
  - 2 For parties to identify each other in the iSHARE framework everyone provides a unique identifier. (EORI number is used to create that).
  - 3 For client identification, all parties use access tokens
-  **x5c** – parameter is a string representing a public key of the certificate to verify signing and identity. It is used by a client as a proof of their identity claim ("client assertion") to get an access token.
-  A request in iSHARE must always be signed by a certificate for QESeal issued by a Trusted Service Provider (TSP) under eIDAS.
-  The identity on the certificate that is used to sign the client assertion should match with the party identifier (EORI).

Source: Data Sharing Coalition analysis based on [iShare Trust Framework v1.10](#)

40 Identity Assurance Framework SCSN. November 2022. Data Sharing Coalition. All rights reserved.



## Two Validation Steps before access token is issued:





# SBR Nexus's use cases rely on eHerkenning and PKI-Overheid certificates for identity assurance



eHerkenning

## Introduction to SBR Nexus

- SBR Nexus is a cooperative initiative of ABN AMRO, ING and Rabobank.
- It provides the standard for digital exchange of business reports based on XBRL (eXtensible Business Reporting Language)
- It ensures the exchange of real estate and financial data (such as credit and annual reports) between companies and banks in a standardized manner through [Mijn Data Mijn Business \(MDMB\) platform](#).

## Key learnings from SBR Nexus for SCSN on LoAs

- In M2M u/c, requiring PKI-Overheid certificates provides stronger identity assurance. This SBR practice can be potentially adopted by SCSN.
- Allowing different levels of eHerkenning in SBR accelerates adoption, since a fit for purpose assurance can be chosen. Similarly SCSN can allow different levels of authentication means to stimulate adoption among Users of different sizes and technical capabilities.

LoA Framework SBR Nexus	General characteristics	<b>Identity owner</b> Natural person Legal person		<b>LoA Issuer</b> Scheme Authority Certified participants Other	
		<b>Liability agreements for mis-use of ID</b> Yes No		<b>LoA is shared in the network by</b> eHerkenning login means	
	LoAs used	Typical u/cs per LoA	U/c Risks	Identification process	Authentication means
Machine-2-Machine (M2M)	Company A uses reporting software to send data to the Bank B via automated link supported by SBR Nexus infrastructure	Financial Reputational Compliance	User follows the process of the Trusted Service Provider to obtain PKI-Overheid service certificate regulated under eIDAS	PKI-Overheid Certificate under eIDAS regulation is used to authenticate a user and provide them with an access token	
Human-2-Machine (H2M)	Accountant representing company A sends a financial report to the Bank B directly via SBR Nexus MDMB platform (this is done via user interface)	Financial Reputational Compliance	User follows the eHerkenning identification process at one of the eHerkenning suppliers  (Note that in some cases iDIN means can be used by physical persons that want to use SBR)	eHerkenning login means depending on the assurance level	

**Legend:** In Scope Not Applicable

SBR Nexus requires their Users to have **eHerkenning of at least EH2+** level, (higher levels EH3, EH4 are supported)

# In M2M cases SBR Nexus requires Users to have PKIoverheid certificate to ensure stronger identity assurance



## The Role of PKIoverheid in M2M use-cases of SBR Nexus

- SBR Nexus uses PKIoverheid certificates to identify, authenticate, and authorise parties. By using private and public keys inside their PKI certificates Users obtain access tokens that enable them to exchange messages and data in the SBR environment.
- There are 3 Qualified Trusted Service Providers (QTSPs), from whom one can obtain PKI certificate for SBR Nexus.

## A process of obtaining PKIoverheid Certificate from a QTSP

### 3 Steps to obtain PKIoverheid 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 PKIoverheid Certificate

QTSP will deliver your certificate by email.

### SBR requires 2 types of PKIoverheid certificates:

**Services Server Certificate**  
(For using SBR Infrastructure (BIV) to send data to banks)

**Digipoort Private Certificate**  
(For using Digipoort to send data to governmental authorities)



## A process of using PKIoverheid Certificate within SBR Nexus

### Setting up PKIoverheid within SBR Nexus:

#### Installations and Checks:

*Inhouse Installations:*

- Intall PKIoverheid certificate in your browser and financial reporting software package

*SBR Nexus "Aansluiten Portal":*

- Go to SBR Aansluiten Portal and fill in the details to register the company and your contact person
- Apload PKIoverheid certificate to the SBR Aansluiten Portal

*SBR Nexus "Acceptance Environment"*

- Run technical tests in the SBR Acceptance Environment, to ensure all runs smoothly.\*\*

#### Usage:

- After the technical checks certifiatue within SBR, can be used to generate JWT access tokens to send/receive financial data.

Note: \* Steps may sliaghtlv varv dependina on the QTSP: \*\* In case of issues reach out to SBR Service Desk

**Sources:** Data Sharing Coalition analysis based on <https://www.sbrnexus.nl/filemanager/uploads/documenten/handleidingen/201903-handleidingPKI.pdf> and <https://www.sbrnexus.nl/mdmb>

# IDSA has Certification Authority (CA) to monitor LoA and certification of participants and their core components

Introduction to IDSA		Key learnings from IDSA for SCSN on LoAs			
<ul style="list-style-type: none"> <li>IDSA is a non-profit coalition with more than 130 member companies.</li> <li>It aims at open, federated data ecosystems ensuring data sovereignty, uniting the requirements from various industries.</li> <li>The IDS certification scheme encompasses all processes, rules and standards governing the certification of participants and core components within the Industrial Data Space.</li> </ul>		<ul style="list-style-type: none"> <li>To ensure on the one hand a low entry barrier specifically suitable for SMEs and on the other hand a scalable certification to meet high information security requirements, the matrix certification approach was defined for the certification of participants.</li> </ul>			
<b>General characteristics</b> <b>Identity owner</b> <input type="checkbox"/> Natural person <input checked="" type="checkbox"/> Legal person <b>Liability agreements for mis-use of ID</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		<b>LoA Issuer</b> <input checked="" type="checkbox"/> Scheme Authority <input type="checkbox"/> Certified participants <input type="checkbox"/> Other <b>LoA is shared in the network by</b> <input checked="" type="checkbox"/> IDS certification			
<b>LoAs used</b>		<b>Typical u/cs per LoA</b>	<b>U/c Risks</b>	<b>Identification</b>	<b>Authentication</b>
LoA Framework IDSA	Participant	Participants (Users) in IDSA either exchange data (entry level and member level participants) or supply different services to support data sharing within IDSA (central level participants)	<input checked="" type="checkbox"/> Financial <input checked="" type="checkbox"/> Reputational <input type="checkbox"/> Compliance	Onboarding goes through 3 stages: application, evaluation, certification <i>But different processes per level:</i> Entry – self-assessment Member – management system Central – control framework	x.509 Digital Certificate issued by Certification Authority of IDSA (containing country name, organization name, UUID (Universally Unique Identifier) and DNS entries/IP Address for the connector)
	Core component	Note that according to IDSA Architecture Model 3.0 each Participant is supposed to have a working connector (core component) attached and certified together with that participant to enable data sharing	<input checked="" type="checkbox"/> Financial <input checked="" type="checkbox"/> Reputational <input type="checkbox"/> Compliance	Onboarding goes through 3 stages: application, evaluation, certification <i>But different processes per level:</i> Base – checklist approach Trust – concept review Trust + – high assurance evaluation	

Source: Data Sharing Coalition analysis based on <https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf>

# Gaia-X focuses on M2M interactions where trust is assured by wallets with verifiable credentials issued by trusted parties



## Introduction to Gaia X

- Gaia-X is a not-for-profit aimed to organise federated infrastructure linking many service providers and users in a transparent environment to drive the future European data economy. IDSA is a founding member.
- Gaia-X has 4 core elements: Federation Services, Standards, Data Spaces and Business Services. The framework can be deployed on top of any existing cloud platform adhering to the Gaia-X standard.

## Key learnings from Gaia X for SCSN on LoAs

- Gaia X plan on implementing wallets with verifiable credentials under eIDAS gives flexibility to Users on which credentials to obtain and use, since specific credentials are based on what service is required. This stimulates adoption.
- Use of ISO and GLEI during the onboarding helps to ensure legal entities can be properly identified

LoA Framework Gaia X	General characteristics	Identity owner	Liability agreements for mis-use of ID	LoA Issuer	LoA is shared in the network by
			Natural person   Legal person	Yes   No	Scheme Authority   Certified participants   Other
	LoAs used	Typical u/cs per LoA	U/c Risks	Identification	Authentication
	Machine-to-machine (M2M) (as defined in the trust doc)	u/c's are domain specific, but they all fit the formula of: "Data service consumer requests data from a data service provider"	Risks vary per domain	<ol style="list-style-type: none"> <li>1. Official company registration number</li> <li>2. Physical location of head quarter in ISO 3166-1 alpha-2, alpha-3 or numeric format.</li> <li>3. Physical location of legal registration in ISO 3166-1 alpha-2, alpha-3 or numeric format.</li> <li>4. Unique LEI (legal entity identifier) from Global Legal Entity Identifier Foundation (<a href="https://www.gleif.org">GLEIF</a>)leif.org</li> <li>5. Parent organisation code, listing a direct participant that this entity is a sub-organization of, if any.</li> <li>6. Sub organization code, listing of direct participant with a legal mandate on this entity, e.g., as a subsidiary.</li> </ol>	Self-description wallet with W3C verifiable credentials in the JSON-LD format, which are issued by TSPs and contain cryptographic signatures
	Human-to-machine interaction is not yet defined	<div style="border: 1px solid green; padding: 2px; display: inline-block;">Non-exhaustive</div> (live examples: Catena X in automobile sector, Agri-Gaia in agricultural sector, Future Care Platform in healthcare sector)		Among different credentials, eIDAS certificates for eSignatures are used	

**Source:** Data Sharing Coalition analysis based on <https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf>  
<https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-Trust-Framework-22.04.pdf>

# Table of contents

1. Introduction Case Study
2. Key Findings Analysis
3. Proposed LoA Framework
4. High Level Roadmap for Execution
- 5. Research Appendix:**
  - Background information on SCSN network
  - Interviews with SCSN network participants
  - Research on assurance in data sharing initiatives (iShare, SBR Nexus, Gaia-X, IDSA)
  - Research on assurance means regulated under eIDAS (eHerkenning, PKI-Overheid, QESeals)

# Steps for a legal person to obtain eIDAS Qualified Digital Certificate for Electronic Seal

Non exhaustive list of Trusted Service Providers per country



## Process of getting eIDAS Qualified Digital Certificate for QESeal

- In order to electronically seal documents as a legal person, a digital certificate for electronic seals is needed.
- Using this certificate and a seal creation device, electronic seals can be created.
- As part of the eIDAS Regulation, these certificates can be purchased from specific providers, named Qualified Trust Service Providers (QTSP).
- Following below is a 3-step process for obtaining the QESeal.

### Step 1: Choose your QTSP from a Trusted List

Go to the eIDAS [Trusted List Browser](#). From this list find and choose a Qualified Trust Service Provider (QTSP). (These providers are granted a qualified status by a national competent authority).

### Step 2: Complete the application process specified by your QTSP

Complete all the actions that the QTSP requires you to do in order to obtain a Qualified Digital Certificate (i.e. proving your identity, paying a service fee).

### Step 3: Obtain a Qualified Digital Certificate for QESeal from a QTSP

Once you have a digital certificate for electronic seal, you will be able to seal your documents. It is done by using the private key included inside the certificate. Providers of qualified certificates for eSeals deliver the corresponding private key on a qualified seal creation device (QSCD).\*

\* QTSPs might offer their own step-by-step process for sealing digitally.

Source: Data Sharing Coalition analysis based on <https://ec.europa.eu/digital-building-blocks/wikis/display/ESIGKB/How+can+I+create+an+advanced+or+qualified+electronic+seal>

# eHerkenning covers H2M use cases in which a Human representative of a company is authenticated

\* Coordinated Vulnerability Disclosure is in place via National Cyber Security Centre (NCSC);

## Introduction to eHerkenning

- eHerkenning is a trust framework that allows authorized users to authenticate their identity on behalf of a company.
- eHerkenning is a login means approved in Europe. It enables representative employees to arrange their company affairs online with government or private organisations in the European Economic Area (EEA) that offer [European login options](#).

## Key learnings from eHerkenning for SCSN on LoAs

- For SCSN, eHerkenning is only relevant in use cases where Human-to-Machine interactions take place. In those cases, eHerkenning and the underlying eIDAS framework enable Relying Parties to authenticate the user

See next slide on how to obtain eHerkenning means from certified parties

General characteristics	Identity owner		LoA Issuer	
	Natural person	Legal person	Scheme Authority	Certified Participants
Liability agreements for mis-use of ID		LoA is shared in the network by		
Yes		No	eHerkenning means	
LoAs used	Typical u/cs	Risks in u/c	Identification criteria	Authentication means
EH2 (eIDAS: basic)	<b>Not applicable:</b> Relying Party decides which LoA to use dependent on their use case risks. eHerkenning provides the guidelines per LoA.		1. Copy of a legal ID document 2. Chamber of Commerce extract no older than 14 days 3. Online application with approved supplier, based on reliable source document	• Login with user-name and password
EH2+ (eIDAS: Basic)			1-3. Same as in EH2 4. Signed application form (if applied via post)	• 2FA login (user-name & password, activation code via SMS, or PIN via a physical token)
EH3 (eIDAS: substantial)			1. Legal ID document (no copy) and face-to-face check. 2-4. Same as in EH2+	• 2FA login (user-name & password, activation code via SMS, QR app, or PIN via a physical token)
EH4 (eIDAS: high)			1-4. Same as in EH3 5. If a party has a qualified certificate, it is used to sign an application, no additional identification is needed then	• PKI qualified certificate or 2FA

Source: Data Sharing Coalition analysis based on <https://www.eherkenning.nl/en/levels-of-assurance>

Legend

In Scope

Not Applicable

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



## Steps 1-3 cover decisions for applying for eHerkenning



### Step 1:

**Decide on service providers you want to log into**

**More than 500**

different service providers (i.e. governmental and private organizations) allow you to login with eHerkenning.

[Check this list](#) to see which service providers you intend to connect to with eHerkenning.



### Step 2:

**Decide who will represent the company using eHerkenning**

Single eHerkenning means with the accompanying authorisations are linked to one individual only.

You need to issue eHerkenning means individually for each representative. But it is possible to apply for them in bulk.



### Step 3:

**Decide on the needed level of assurance out of 4 levels:**

**EH2 EH2+ EH3 EH4**

The service provider determines the LoA required for their online services.

If you intend to use multiple services, better opt for the highest level.\*

\*Note: if needed the level can be upgraded later on

## Steps 4-6 describe the actions for obtaining eHerkenning



### Step 4:

**Authorise each individual representative**

The authorisation specifies for which service providers, and for which services, an individual can log into on behalf of their organisation.

Two people grant an authorisation:  
**Authorised signatory**  
**Authorisation manager**



### Step 5:

**Select a trusted supplier and apply for eHerkenning**

**6 official suppliers**

of eHerkenning can identify you and provide login means based on the assurance level you choose.



### Step 6:

**Activate eHerkenning means and start using them**

Once you have purchased eHerkenning login means\*, you can activate and use them.

\*Overview of login means per assurance level:

<b>EH2</b>	Username & password
<b>EH2+</b>	2FA
<b>EH3</b>	2FA
<b>EH4</b>	PKI certificate or 2FA