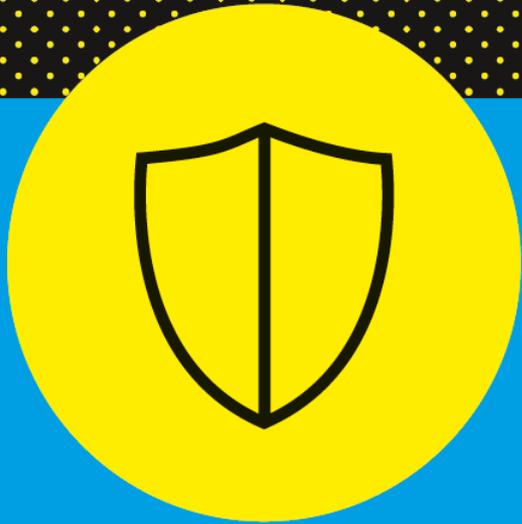




# How to get IDS\_certified

Road to become a  
partner in a data ecosystem

Live Session  
October 28 | 11 a.m. (CET)



## AGENDA

### Introduction

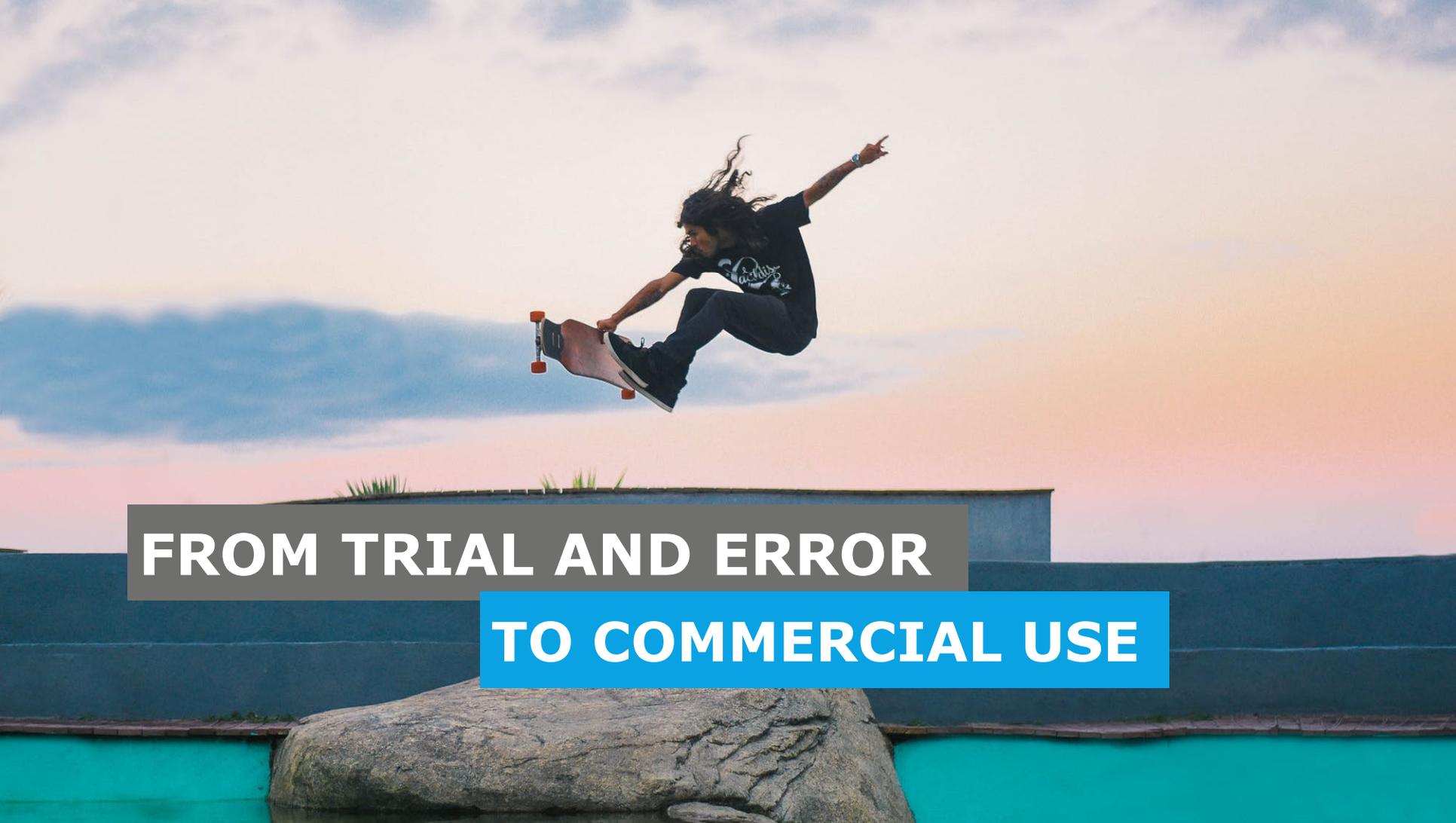
*Lars Nagel, CEO IDSA*

### What does IDS Certification mean?

*Sebastian Steinbuss, CTO IDSA*

### How to get certified?

*Natalia Simon, Project manager IDSA*



**FROM TRIAL AND ERROR**

**TO COMMERCIAL USE**



# **IDSA looks back on five years of paving the way for a sovereign data economy in Europe and globally. Now, IDS is ready to use.**

IDSA has defined a reference architecture and a formal standard for creating and operating virtual data spaces. The IDS Architecture ensures data sovereignty for data owners making data available for being exchanged and shared.

## ***What is so special now?***

1. We make the IDS Connector for business transactions in data ecosystems available;
2. we define the governance rules for these transactions;
3. we certify the participants of these transactions.

With these three pillars, IDS is the basis for innovative business models and data ecosystems. It establishes the right to data sovereignty in the digital age.



# What is so special now?

## *Certification*

Participants and components of IDS-based data ecosystems must provide a high degree of trust and security regarding the integrity, confidentiality and availability of data.

Using certified components and employing certified technical and organizational security measures is mandatory for participating in the IDS.

The IDS Certification Scheme defines security levels for components and the requirements to be implemented.

**Five evaluation facilities are ready to award the IDS\_certified label.**

## *Rule Book*

IDS is a technological standard and a legal framework to create data ecosystems.

Key requirement to make this a reality is to have a set of rules and policies governing it in a decentralized way.

These rules and policies are contained in the **IDS Rule Book**.

It describes the technical, operational, and legal agreements to enable the IDS ecosystem to be fully working in a real-world scenario.

## *Launching Coalition*

The IDS Launching Coalition is a group of IDSA member companies.

They intensified their engagement to have use cases running and their solutions certified till November 2020.

This is a crucial step to establish the first commercial IDS ecosystems which are based on trust and data sovereignty.

Going live with **commercial IDS-based solutions** will enable data providers from different domains to monetize their data treasures and stay the sovereign of their data.

## *Design Principles for European Data Spaces*

The European Data Strategy creates a vision of data spaces governed by rules that are derived directly from fundamental European values.

**IDS is an indispensable element of European data spaces** – a blueprint for all kinds of data sharing ecosystems and marketplaces based on data sovereignty.

IDSA contributes technology and provides data infrastructure services to the operation of the European data spaces as well as advisory to the European Data Act and a network to support knowledge sharing.

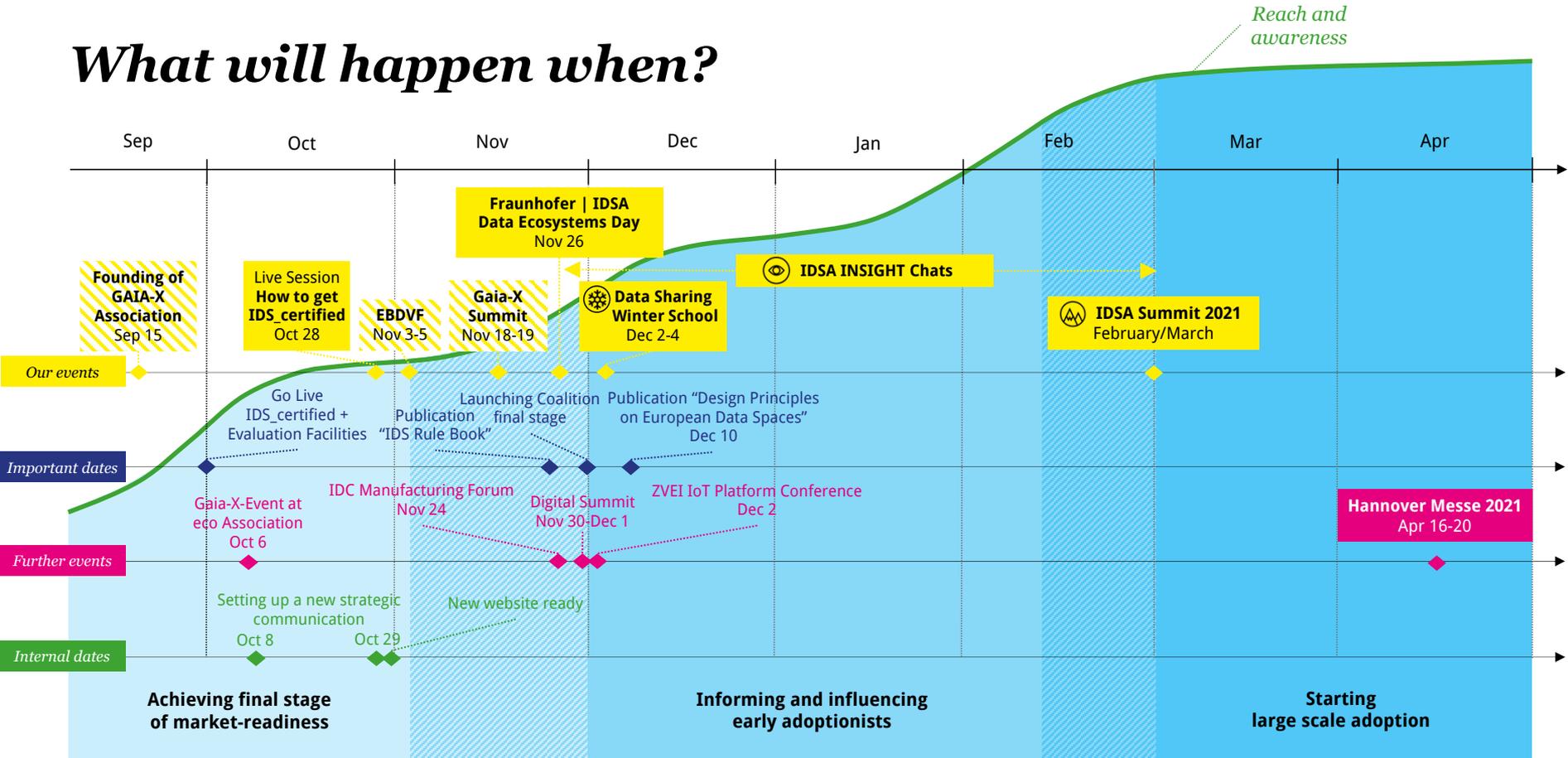
## *Central element for GAIA-X*

The **IDS Reference Architecture on data sovereignty will be a central element of the GAIA-X architecture.**

As a basis for an open ecosystem, it enables providers and consumers of data to connect in a secure, interoperable and sovereign way.

Combined with highly available storage and efficient processing of data GAIA-X has the potential to create a secure and trustworthy data infrastructure based on European values.

# What will happen when?





I Agree

**#datasovereignty**

# DATA TREASURES

ARE CREATED BY SHARING DATA

*Linking data is the new oil of the data driven economy*

*Companies want to share data without regret*

*Stay in control over the flow of your data*



# DATA SHARING REQUIRES

# A COMMUNITY OF TRUST

*Trustworthy identities*

*Crystal clear governance for data sharing*

*Data sovereignty*



*Governance for data sharing*

*Defining usage constraints*

*Trusted manipulation of data*

**DATA SPACES**

**CLEANROOMS FOR A PROSPERING DATA ECONOMY**

# IDS CONNECTOR

ENABLES ACCESS TO SOVEREIGN,  
TRUSTED DATA SHARING ECOSYSTEMS

# 4

**Security profiles**  
satisfying all needs from quick data sharing to comprehensive security requirements



Defined in DIN Spec 27070 on "security gateway for sharing data and services" and reference architecture model 3.0



Specifications for implementing a connector based on container management technologies provided on Gitlab



Implementation in different scenarios (embedded systems, mobile devices, client server solutions)

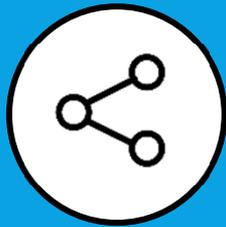


Formal certification states coherence to reference architecture, interoperability and software quality



# DESIGN PRINCIPLES FOR DATA SPACES

## ENSURING DATA SOVEREIGNTY



### Unlimited **Interoperability**

standard for data flows between  
all kinds of data endpoints



### **Trust** between different security domains

Comprehensive security functions  
providing a maximum level of trust

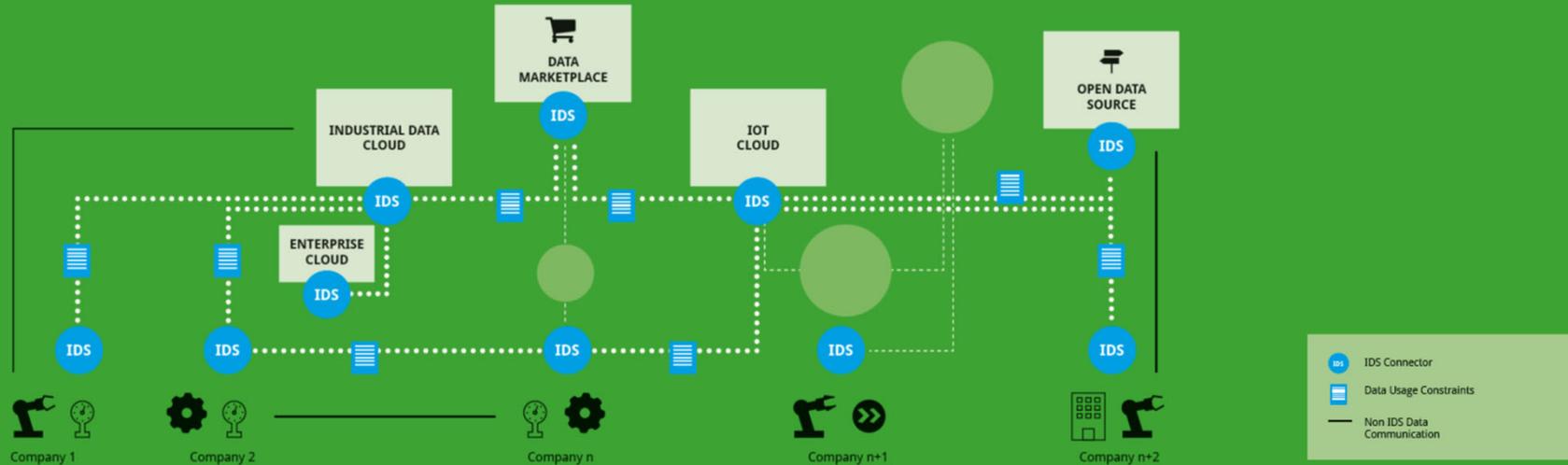


### **Governance** for the data economy

usage control and enforcement  
for data flows

# THE INTERNATIONAL DATA SPACES APPROACH CONNECTS ALL KINDS OF DATA ENDPOINTS

When broadening the perspective from an individual use case scenario to a platform landscape view, the INTERNATIONAL DATA SPACES positions itself as an architecture to link different cloud platforms through secure exchange and trusted sharing of data, short: **through data sovereignty.**



By proposing a specific software component, the INTERNATIONAL DATA SPACES Connector, industrial data clouds can be connected, as well as individual enterprise clouds and onpremise applications and individual connected devices.

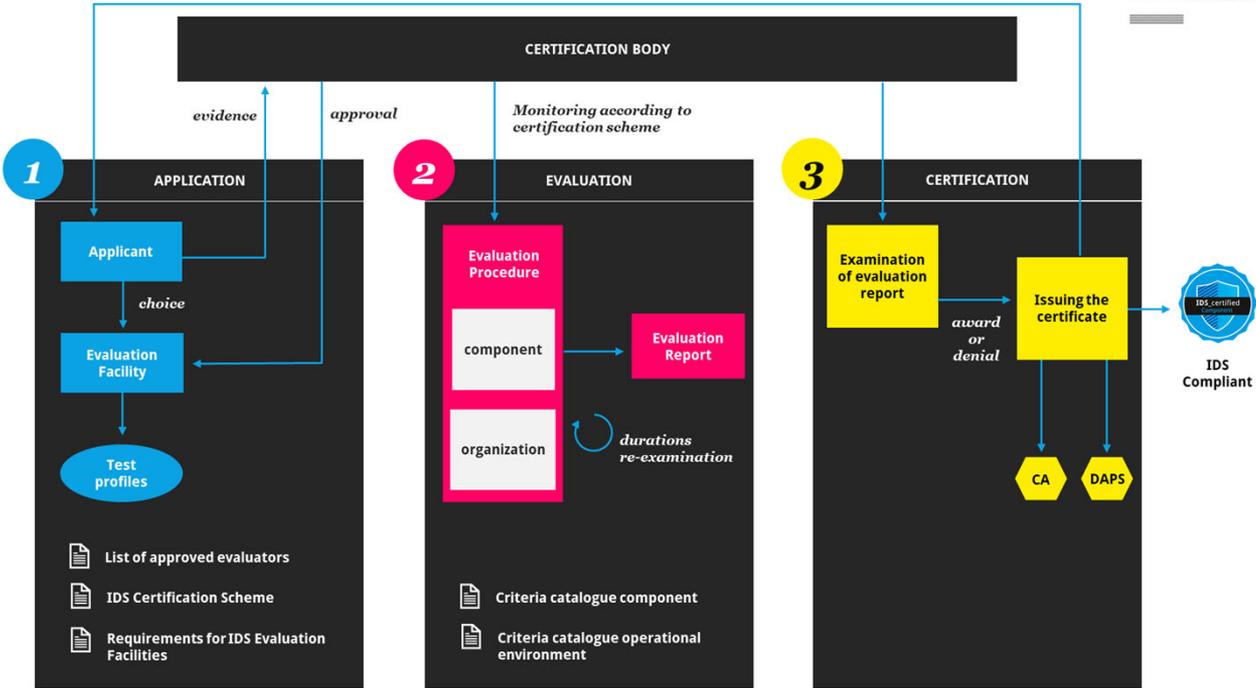


**What does  
IDS Certification  
mean?**

# SETTING UP IDS CERTIFICATION

Certification Body is in place today and realized in the IDSA Support Organization (midterm)

This is the bridge to enable IDS Certification





# SYNERGY OF CERTIFICATES



## Organization Certificate

- IDS-specific organizational criteria (aligned with ISO/IEC 27001) are used
- Existing certificates can be re-used by an organization, if applicable to IDS-relevant scope, e.g.:
  - ISO/IEC 27001:2013
  - CSA Cloud Controls Matrix 3.01
  - BSI IT - Grundschatz 14.EL 2014
  - BSI SaaS Sicherheitsprofile 2014



## Component Certificate

- IDS-specific requirements
- Functional requirements taken from 62443-4-2
- Best practice requirements for secure software development
- Existing 62443 certificates can be re-used by a developer, if applicable to IDS-relevant implementation scope and security level



# OPERATIONAL ENVIRONMENT CERTIFICATION

## Asset Management

- Media shall be disposed of securely when no longer required, using formal procedures.

## Communication Security

- Groups of information services, users and information systems shall be segregated on networks.

## Identity and Access Management

- Asset owners shall review users' access rights at regular intervals.

## Organization of Information Security

- Information security shall be addressed in project management, regardless of the type of the project.

## Physical Security

- Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

## Security Incident Management

- Ensuring a consistent approach regarding the monitoring, recording, assessment, communication and escalation of security incidents.





# SECURITY PROFILES FOR CORE COMPONENTS

## AS SPECIFIED IN CRITERIA CATALOGUE

### Security Levels

Mapping of IEC 62443 to IDS Certification

	Base SecurityProfile	Trust SecurityProfile	Trust+ SecurityProfile
62443-IAC	SL2	SL3	SL3
62443-UC	SL1	SL2	SL2
62443-SI	SL1	SL3	SL3
62443-DC	SL1	SL3	SL3
62443-RDF	SL1	SL3	SL3
62443-TRE	SL1	SL3	SL3
62443-RA	SL1	SL3	SL3
62443-NDR	SL1	SL3	SL3

### Additional Requirements

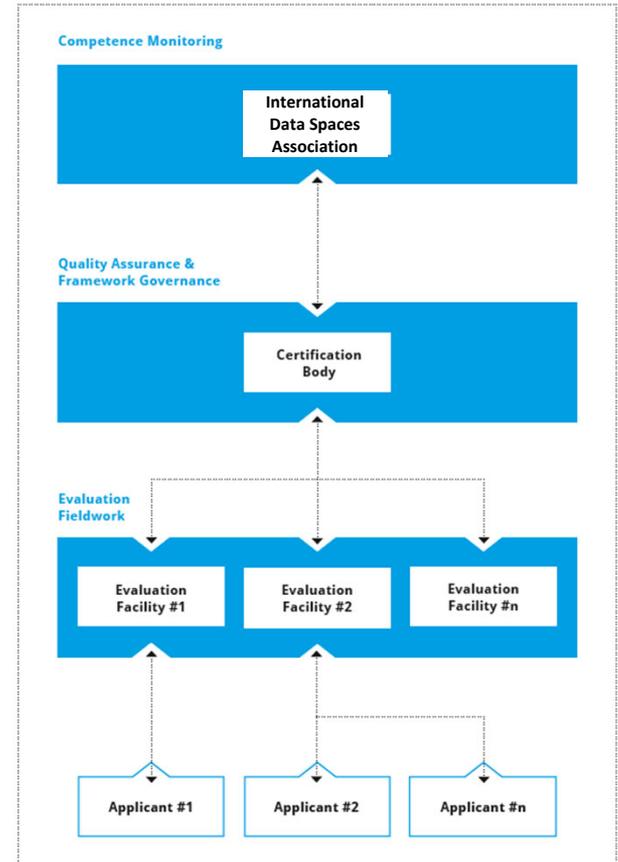
- **Communication security**
  - More detailed requirements for ciphers & crypto
  - Remote integrity verification, remote attestation
- **Data usage control**
  - Information flow control and usage control requirements
- **Information model**
  - Requirements towards the information model and metadata
- **Identity & access management requirements**
  - Certificates, DAPS, ...
- **Broker integration**
  - Broker interaction requirements
- **Operating system security**
- **Audit logging**



# IDS REFERENCE ARCHITECTURE MODEL

## Roles & Responsibilities in IDSA Certification

	Entry Level	Member Level	Central Level
Data Owner	Required	Recommended	Optional
Data Provider	Required	Recommended	Optional
Data Consumer	Required	Recommended	Optional
Broker Service Provider		Required	Optional
App Store Provider		Required	Optional
Vocabulary Provider		Required	Optional
Service Provider		Required	Optional
Clearing House			Required
Identity Provider			Required



# IDS REFERENCE ARCHITECTURE MODEL

## Roles & Responsibilities in IDSA Certification



Operational Environment



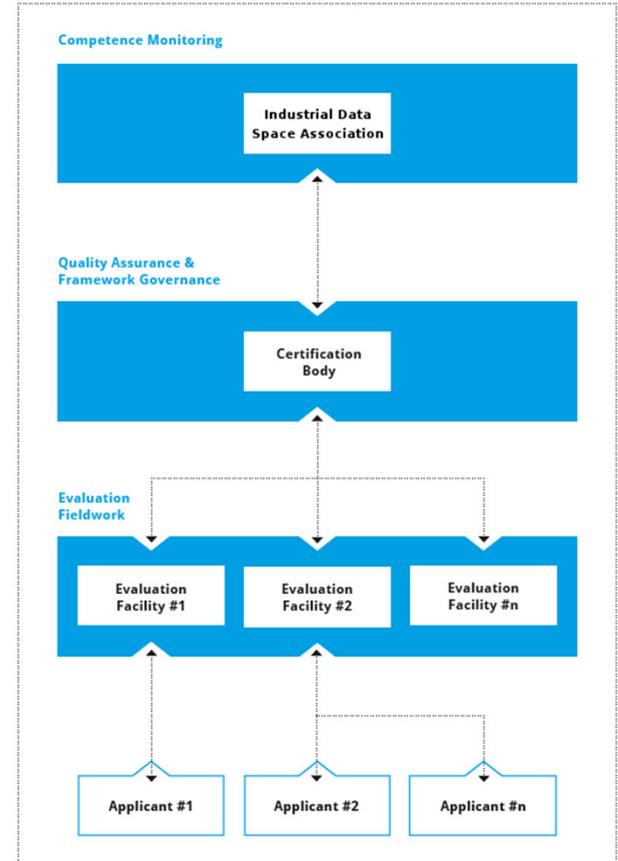
	Self-Assessment	Management System	Control Framework
Entry Level	✓	✓	
Member Level		✓	✓
Central Level		✓	✓



Components



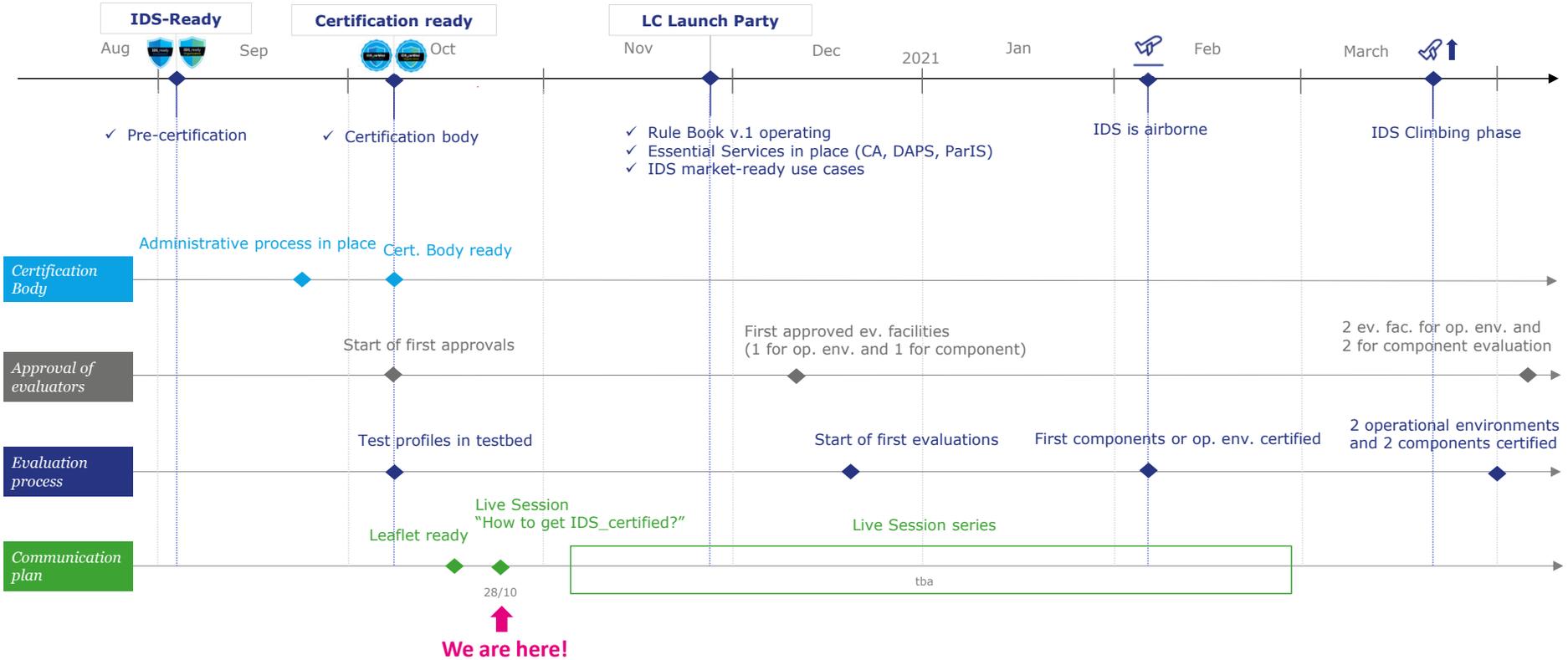
	Checklist Approach	Concept Review	High Assurance Evaluation
Base Security Profile	✓	✓	
Trust Security Profile		✓	✓
Trust+ Security Profile		✓	✓



# IDS CERTIFICATION TIMELINE

LEGEND

◇ Milestone



*The **IDS**A Support Office is your contact point to offer guidance to step into the IDS Certification.*

*This includes the tasks and duties of the Certification Body.*

*For more information see the **IDS**A Rule Book*

**INTERNATIONAL DATA  
SPACES ASSOCIATION**



*[supportoffice@internationaldataspaces.org](mailto:supportoffice@internationaldataspaces.org)*



**Giulia Giussani** | *Digital Innovation Manager*



**Natalia Simon** | *Project Manager*



**How to get  
IDS certified?**

# The Certification Body is in place and ready to approve Evaluation Facilities

To become an Evaluation Facility

1

Contact the Support Office. We will consult you on the process and guide you throughout the steps.

2

Apply at your Certification Body for your specific area of certification.

3

The Certification Body will start the audit process and collaborate with you on collecting all necessary documents and information.

## In the meantime

Prepare for certification by

- Participating in the IDS Plugfest
- Participating in the Integration Camp
- Conducting the IDS ready assessment

We will consult you on the process and help you find the perfect partner.

Onboarding session with your Evaluation Facility. You will get your individual audit road map.

The Evaluation Facility will start the audit process and collaborate with you on collecting all necessary documents and information.

To certify your components / operational environment

1

2

3



**Become an  
IDS Evaluation Facility**

**Apply NOW**

[supportoffice@internationaldataspaces.org](mailto:supportoffice@internationaldataspaces.org)



## ALL THE STEPS WE HAVE ACHIEVED AND THAT WE HAVE AHEAD

1. We have now in place the Certification Body
2. You, if you like to certify your component, you can prepare (Plugfest, Integr Camp, etc.)
3. Meanwhile we are approving the Evaluation Facilities
4. When this is ready, will announce it on the website, then you can certify
  1. Operational environment
  2. Base Connector, Broker
  3. Trust connector
  4. Trust + connector

Support Office is always there to guide you through the process.





# QUESTIONS & ANSWERS

*Raise your hand and we will activate your mic,  
or just write in the Q&A section.*



*“A trusted sharing of data in  
business ecosystem stimulates  
innovation, provides transparency,  
eases processes and  
drives business”*



**Join us!**

## INTERNATIONAL DATA SPACES ASSOCIATION



**Thorsten Hülsmann** | CFO  
*thorsten.huelsmann@internationaldataspaces.org*



**Lars Nagel** | CEO  
*lars.nagel@internationaldataspaces.org*



**Sebastian Steinbuss** | CTO  
*sebastian.steinbuss@internationaldataspaces.org*



**Natalia Simon** | Project Manager  
*natalia.simon@internationaldataspaces.org*

*[www.internationaldataspaces.org](http://www.internationaldataspaces.org)*

# User Journey for Developers

- Service
- Documentations
- Wish-List
- JIVE
- Video
- Members only
- Fee
- Further details on the website
- Not yet available

WORK IN PROGRESS

- 1 Gather knowledge**  
Get a better understanding of the IDS technical concepts and core ideas. Get in touch with the community.
- 2 Design your architecture**  
Consider your company's and ecosystem's requirements. Design your components based on the IDS.
- 3 Develop your components**  
Build your own components from scratch or use existing open source components.
- 4 Integrate your components**  
Integrate your components with those of your partners and other IDS participants.
- 5 Prepare for IDS certified**  
Review the certification criteria. Prepare your code, documentation and environment for the evaluation.
- 6 Get IDS certified**  
Contact an IDS evaluation facility to certify your component or operational environment.
- 7 Register to get on board**  
Provide the required documents and information to the onboarding facility. Set-up your offering and get into the IDS.
- 8 Start sharing**  
Start sharing your data within your ecosystem.



How to Prepare for Certification



CERTIFICATION BODY

evidence

approval

Monitoring according to certification scheme

1

APPLICATION

Applicant

choice

Evaluation Facility

Test profiles

- List of approved evaluators
- IDS Certification Scheme
- Requirements for IDS Evaluation Facilities

2

EVALUATION

Evaluation Procedure

component

Evaluation Report

organization

durations re-examination

- Criteria catalogue component
- Criteria catalogue operational environment

3

CERTIFICATION

Examination of evaluation report

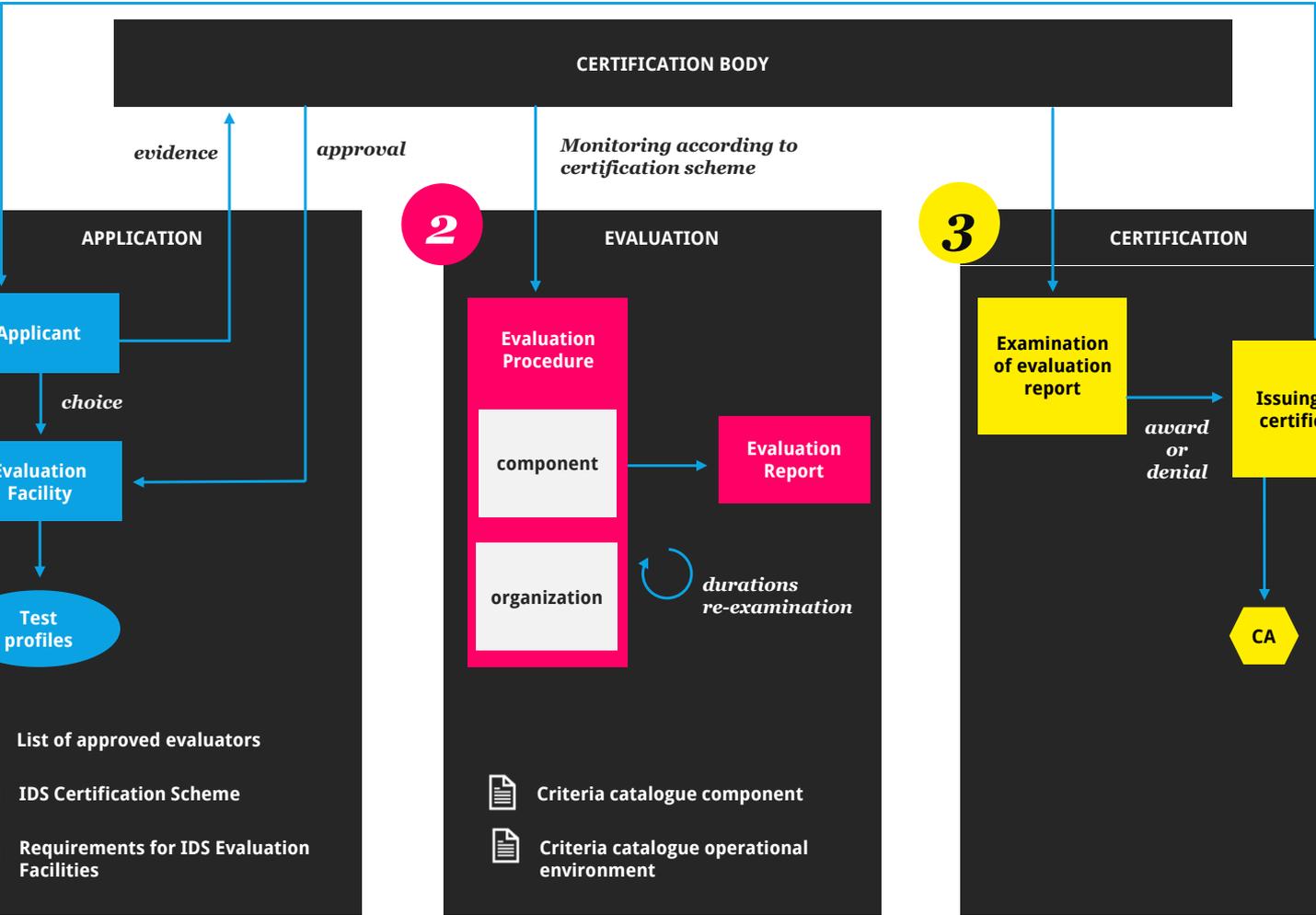
award or denial

Issuing the certificate

CA DAPS



IDS Compliant





# OPERATIONAL ENVIRONMENT CERTIFICATION

	Entry Level	Member Level	Central Level
Data Owner	Required	Recommended	Optional
Data Provider	Required	Recommended	Optional
Data Consumer	Required	Recommended	Optional
Broker Service Provider		Required	Optional
App Store Provider		Required	Optional
Vocabulary Provider		Required	Optional
Service Provider		Required	Optional
Clearing House			Required
Identity Provider			Required



	Self-Assessment	Management System	Control Framework
Entry Level	✓	✓	
Member Level		✓	✓
Central Level		✓	✓



# COMPONENT CERTIFICATION



	Checklist Approach	Concept Review	High Assurance Evaluation
Base Security Profile	✓	✓	
Trust Security Profile		✓	✓
Trust+ Security Profile		✓	✓