Prototyping the IDS Security Components in the Context of Industry 4.0 - A Textile and Clothing Industry Case Study

Nuno Torres[1][0000−0001−7598−3687], Ana Chaves[2][0000−0001−7960−6459], César Toscano[2][0000−0002−6056−6917], and Pedro Pinto[1,2,3][0000−0003−1856−6101]

[1] ADiT-LAB, Instituto Politécnico de Viana do Castelo, Viana do Castelo 4900-348, Portugal

[2] INESC TEC, 4200-465 Porto, Portugal

[3] Universidade da Maia, Maia 4475-690, Portugal

Abstract. With the introduction of Industry 4.0 technological concepts, suppliers and manufacturers envision new or improved products and services, cost reductions, and productivity gains. In this context, data exchanges between companies in the same or different activity sectors are necessary, while assuring data security and sovereignty. Thus, it is crucial to select and implement adequate standards which enable the interconnection requirements between companies and also feature security by design.

The International Data Spaces (IDS) is a current standard that provides data sharing through data spaces mainly composed of homogeneous rules, certified data providers/consumers, and reliability between partners. Implementing IDS in sectors such as textile and clothing is expected to open new opportunities and challenges.

This paper proposes a prototype for the IDS Security Components in the Textile and Clothing Industry context. This prototype assures data sovereignty and enables the interactions required by all participants in this supply chain industry using secure communications. The adoption of IDS as a base model in this activity sector fosters productive collaboration, lowers entry barriers for business partnerships, and enables an innovation environment.

Keywords: IDS; DAPS; Connectors; Security; Industry 4.0.

1 Introduction

Data storage and exchange are essential requirements for companies operating in multiple activity sectors. Corporate services' communications include trade secrets and sensitive data; thus, protecting data integrity, authenticity and confidentiality are mandatory.

The use of Industry 4.0 technological concepts transforms how businesses produce, enhance, and distribute their products while reducing costs and enhancing their productivity. Thus, selecting and implementing adequate standards featuring security by design is of utmost importance. Using a standard that provides secure data sharing is a good solution for the industrial context, which still lacks implementation guides from the beginning until the end of the deployment.

International Data Spaces (IDS) is a recent standard that provides data sharing through data spaces mainly composed of homogeneous rules, certified data providers/consumers, and reliability between partners. Its primary goal is to ensure secure and standardized data exchange and linkage in a trusted business ecosystem while facilitating cross-company business processes and guaranteeing data sovereignty for data owners.

This paper proposes a prototype based on IDS for the textile and clothing sector. The communication between participants is provided by connectors and their interaction with an identity provider, as defined by the IDS. The prototype was implemented in the context of the mobilizing project Digitization of the Textile and Clothing Sector Value Chain (STVgoDigital) [1], where a set of partners in this activity sector are characterized by production orders and availability status from an industrial organization to its subcontractors. Thus, the implementation herein provided can be relevant for any set of organizations in this activity sector and other similar activity sectors, enabling all the required interactions between the companies involved in the supply chain.

The remaining document is organized as follows. Section 2 presents the related work. Section 3 presents the security-related key concepts of the IDS architecture and describes its security components Section 4 describes the prototype implementation. Section 5 presents a discussion regarding the prototype implementation. Section 6 presents the conclusions.

2 Related Work

The concepts of Security-by-Design and Privacy-by-Design imply that the principles of security and privacy of data and messages in a communication system are implemented and assured from the project's beginning to its end. In [2], a Security-by-Design model for Industry 4.0 is proposed, which aims to minimize system vulnerabilities and reduce the surface of attacks by ensuring security construction in every stage of the Software Development Life Cycle (SDLC). The authors divide security into three phases: the identification of security requirements, the identification of security risks and the security measures, which are divided based on software and hardware.

One of the reference modules for Industry 4.0 is the Reference Architecture Model Industry 4.0 (RAMI 4.0). It features a service-oriented model which combines all technological elements and components in a single model of layers and life cycles. RAMI 4.0 is divided into three axles: architecture, life cycle value flow and hierarchy, and finally, the inclusion of data privacy and security mechanisms [3]. In [4], a perspective towards the security of RAMI 4.0 is approached, where it is identified two sets of enablers: Smart Networking to facilitate the connection of internal logistics; and automatized systems, which utilize Cloud-based frameworks to control the system point-to-point, report failures, and connect final users to suppliers practically and efficiently. The article [5] proposes an architecture model for Industry 4.0, based on RAMI 4.0 model, to monitor a production environment. It also presented a case study that considers good practices in the security of networks, systems and information, leading to the development of an architecture with generic use, processes, communications and data management, all based on the Cloud. In [6], the authors propose an end-to-end communication model for cyber-physical systems based on RAMI 4.0. This model is auto-adaptive to improve the trade-off between the performance of business processes and end-to-end communication safety. A recent effort is realized involving the IDS initiative that vices independent data sharing and control, guaranteeing the safety and sovereignty of data. In the article [7], the authors explored the technical architecture of GAIA-X, including the security perspective. From the security perspective, several approaches are made, from defining security-by-design and privacy-by-design as development guidelines to determining that openness, transparency, authenticity, and trust are core objectives of the architecture. In [8], the authors approach IDS from a security perspective. They identified that infrastructures must be equipped with components, such as identity managers or dynamic trust managers, to guarantee data sovereignty. Users must be certified (X.509) to participate in the data exchange, to which some restrictions on the use of data may be enforced to guarantee privacy [9] through the IDS connector, and this way, safely sharing data between parties. In [10] are presented works in progress towards implementing the IDS architecture for a heterogeneous Internet of Things (IoT) communications devices scenario. Using IDS is the leading choice for sharing data between participants. This report also presents a design for an IoT-Connector that acts as a communication interface between IoT devices and IDS connectors. In [11], the authors evaluated a real-time sovereign data exchange in IoT devices. The communication schemes were proposed and implemented following the IDS guidelines. Results showed benefits in the publish/subscribe version in longer operation times, allowing to enter low-power mode, while request/response performed better on short operations. The article [12] proposed an approach to enable the IDS for vendor-independent IoT devices, allowing data owners to benefit from providing their own data while retaining control over it. In [13] is presented an industrial scenario that simulates manufacturing as a service system for the execution of remote production orders based on the implementation of IDS connectors. The article presents a use case where IDS connectors are used in a manufacturing context and where remote production orders are securely performed. In [14], a smart factory web platform is discussed and extended by implementation with the current state of the IDS. The evaluation showed that the base connectors' communication works due to the standardized protocols and security mechanisms being re-used. In [15], the authors introduced an enterprise architecture to help companies choose which organizational and software components to implement before entering an IDS ecosystem. This paper also promotes a better understanding of the guidelines provided by the International Data Spaces - Reference Architecture Model (IDS-RAM) for companies interested in joining IDS ecosystems.

3 IDS Security Architecture and Components

The IDS architecture [16] specifies seven key concepts to achieve security: (1) secure communications, (2) identity management, (3) trust management, (4) trusted platform, (5) data access control, (6) data usage control, and (7) data provenance tracking. These key concepts are detailed as follows.

1. Secure Communications - The communication between connectors must be protected to ensure authenticity and confidentiality in data transfer. When using an IDS connector, there are two layers of security: 1) Point-to-point (between connectors) encryption, achieved through the use of a tunnel, and 2) End-to-end authorization (authorization and authenticity based on current communication endpoints). IDS connectors must communicate with each other through an encrypted tunnel (Transport Layer Security (TLS)) and must also use another appropriate protocol, such as Hyper Text Transfer Protocol Secure (HTTPS).
2. Identity Management - To control the accesses of participants, with their trusted identities and properties, a concept for Identity and Access Management (IAM) is mandatory with the following functions: Identification (claim an identity), Authentication (verify an identity), and Authorization (make access decisions based on identity). The Certification Authority (CA) issues certificates for all entities. These certificates are used for authentication and encryption between connectors. An identity could contain several attributes which are connected to the identity itself. The Dynamic Attribute Provisioning Service (DAPS) provides dynamic and updated information about the participants and their connectors.
3. Trust Management - To establish trust across the entire ecosystem, IDS uses cryptography methods. One of the methods is Public Key Infrastructures (PKI). A central concept of a PKI is that all entities are allocated with secret keys, allowing each entity to authenticate regarding other participants. Therefore, a hierarchy is created, with the Identity Provider at the top issuing certificates to other entities. Additionally, the trust regarding the creation and sharing of data in an IDS ecosystem should be strengthened through certifications assigned to the software components used to implement a data space.
4. Trusted platform - The IDS consists of multiple instances of the connector-based architecture. The trusted platform is a core element of the trusted data exchange and includes the following functions, namely, (1) to specify the minimum requirements for participants that want to exchange data and provide mutual verification of the security profiles of the participants, (2) to enable reliable execution of data applications and ensure system integrity, i.e. the Data Apps only have access to the data that is explicitly intended for them, and (3) to provide a remote integrity verification and establish a trust relationship with another Participant, with verification of the connector's properties.
5. Data access control - IDS defines access control as a resource-centred regulation of access requests from the IDS participants to resources (Data Services).

Data owners define attribute-based access control policies for their endpoints and the values of attributes a subject must satisfy to guarantee access to the resource. These attributes include (1) the identity of the connector(s) (only access requests from one or more specific connectors will be guaranteed), (2) Connector attributes (only access requests from a connector with specific attributes will be guaranteed), (3) security profile requirements (only access requests from a connector that satisfies specific security requirements will be guaranteed).

6. Data usage control - The usage control is an extension of access control and it specifies and enforces the restrictions regulating how the data is managed and what is the data consumer obligations [17]. It allows Data Providers to attach data usage policies to their data to define how a Data Consumer may use it. Usage control is a transversal concept and technology which involves the following IDS functions:
   - Broker: The IDS Broker maintains connector self-descriptions and metadata descriptions that describe the data sets provided and consumed by the Data Provider and Data Consumer entities in the context of an IDS. In this context, data usage policies can also be identified.
   - Connector: The connector is the central technical component for implementing the IDS infrastructure and is responsible for every communication inside the ecosystem. Moreover, connectors that work as Data Providers must provide technology-dependent policies for the data provided - for all types of application systems and technologies that are part of the ecosystem.
   - Clearing House: By tracking the origin of the data, it is possible to follow its use and compliance with the usage restrictions. The Clearing House can use this data later for auditing purposes.
7. Data provenance tracking - Data provenance tracking is closely related and complementary to distributed data usage control. It allows knowing when, how, and who modified the data and which data influenced the process of creating new data. This type of traceability is similar to the data protection requirements with which a data controller is faced in order to be able to fulfil the right of access to its data subjects. It is also related to the issue of proving compliance with contracts, agreements, or legal regulations. Additionally, it can facilitate the aggregation of information about data exchange transactions and data usage in a decentralized data ecosystem.

In order for IDS to assure data integrity, authenticity and confidentiality, two security components of the IDS are required: Connectors and an Identity Provider.

The connector is the central IDS component, serving as a bridge to connect existing systems and their data with the rest of the ecosystem. Its architecture and functionalities are defined by the IDS-RAM [16] and specified by the certification criteria. The connector allows data exchanges with other connectors and the data could be enriched with metadata. The Dataspace Connector [18] is an open-source implementation created by Fraunhofer ISST[4]. It uses the most recent version of the IDS Information Model[5] and the IDS Messaging Services[6] to handle messages made with other IDS components. External data sources can be connected via Representational State Transfer (REST) endpoints, allowing the Dataspace Connector to act as an intermediary between the IDS data ecosystem and the real data source. According to the requirements of a data space, communications with other IDS connectors, encrypted via TLS, and communication with an IDS Broker, are supported in the context of an IDS data ecosystem. The Dataspace Connector can simultaneously act as a data consumer and provider, providing data to an IDS ecosystem and requesting data from other IDS connectors.

The Identity Provider offers a service that allows the creation, maintenance, management, monitoring, and validation of the information identity from and for the IDS participants. Which is strictly necessary to ensure the security of IDS operations and prevent unauthorized data access. The Identity Provider is comprised by:

- Certification Authority - manages the IDS participants' digital certificates.
  - The CA is responsible for issuing, validating, and revoking digital certificates. A digital certificate is provided to a participant if both the participant and core component (i.e., connector) certificates are valid and available. The CA provides an IDS-ID for a combination of the participant and main component. The digital certificate is valid, not exceeding the validity of both certifications, i.e., the participant certification and the certification of the main component used by the participant. This component only provides the X.509 digital certificate to the participant if requested, securely sending it and notifying the DAPS. The Certification Authority is also responsible for issuing certificates to all entities, which are then used for authentication and encryption between connectors.
- Dynamic Attribute Provisioning Service - service that manages the dynamic attributes of the participants.
  - A digital identity relies on different attributes which are linked to that identity. The DAPS provides dynamic and up-to-date attribute information about participants and connectors. It was developed to enrich participants and connectors with attributes embedded into a Dynamic Attribute Token (DAT). The resulting information from the certification process is transmitted to DAPS, which includes master data and information about security profiles. The CA provides the details of the digital certificate (public key and IDS-ID). The participant is registered on the

[4] `https://www.isst.fraunhofer.de/en.html`

[5] `https://international-data-spaces-association.github.io/InformationModel/docs/index.html`

[6] `https://github.com/International-Data-Spaces-Association/IDS-Messaging-Services`

DAPS after successfully implementing the digital certificate within the component.

- Participant Information Service - registry for self-description documents of IDS Participant.
    - This component is responsible for making the Participants' information available, enabling business interaction between unrelated Participants. This component works as a central catalogue of information. Furthermore, as its goal is to make information available, it is mainly used by companies that have yet to work together and therefore do not trust each other. A verifiable identity management process achieves that trust through the Identity Provisioning Service and the DAPS. Both components equip each participant with the necessary attributes and cryptographic proofs for the IDS handshakes.

4 Prototype Implementation

The current research work was developed based on a scenario from a mobilising project named STVgoDigital which was intended to digitise the value chain of the Textile and Clothing Sector. The current implementation fits the project's objective and promotes the adoption and transition to the digital transition to the textile and clothing activity sector and other similar activity sectors.

The prototype implementation comprehended 4 stages: (1) definition of the requirements and architecture, (2) components configuration, and (3) communication testing. These stages are detailed as follows.

4.1 Requirements and Proposed Architecture

The scenario for an IDS ecosystem should be defined as the architecture depicted in Fig. 1. The architecture should comprehend the following items:

- Connector 1 - Facility A (Consumer)
- Connector 2 - Facility B (Provider)
- DAPS - Consortium Management Company (DAPS Server)
- Certification Chain - (via CA)
- Governance Body - Consortium Management Company (Certification Body + Evaluation Facility)

Connector 1 and Connector 2 should be installed in two different facilities. The DAPS server should be installed on the Consortium Management Company. The Certification Chain may be deployed through an external service responsible for the maintenance of the CA. The Governance Body should be deployed in the Consortium Management Company since it will be responsible for validating the participants' identities and verifying if they correspond to the facilities associated with the IDS.

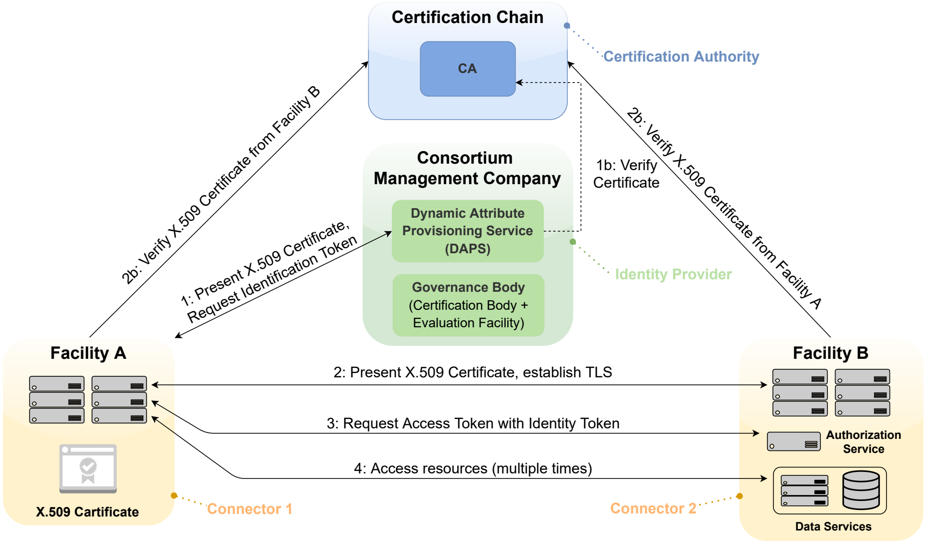
Certification Chain
CA
Certification Authority
Consortium Management Company
Dynamic Attribute Provisioning Service (DAPS)
Governance Body (Certification Body + Evaluation Facility)
Identity Provider
1b: Verify Certificate
2b: Verify X.509 Certificate from Facility B
2b: Verify X.509 Certificate from Facility A
1: Present X.509 Certificate, Request Identification Token
Facility A
X.509 Cartificate
Connector 1
Facility B
Authorization Service
Data Services
Connector 2
2: Present X.509 Certificate, establish TLS
3: Request Access Token with Identity Token
4: Access resources (multiple times)

Fig. 1. Proposed Architecture

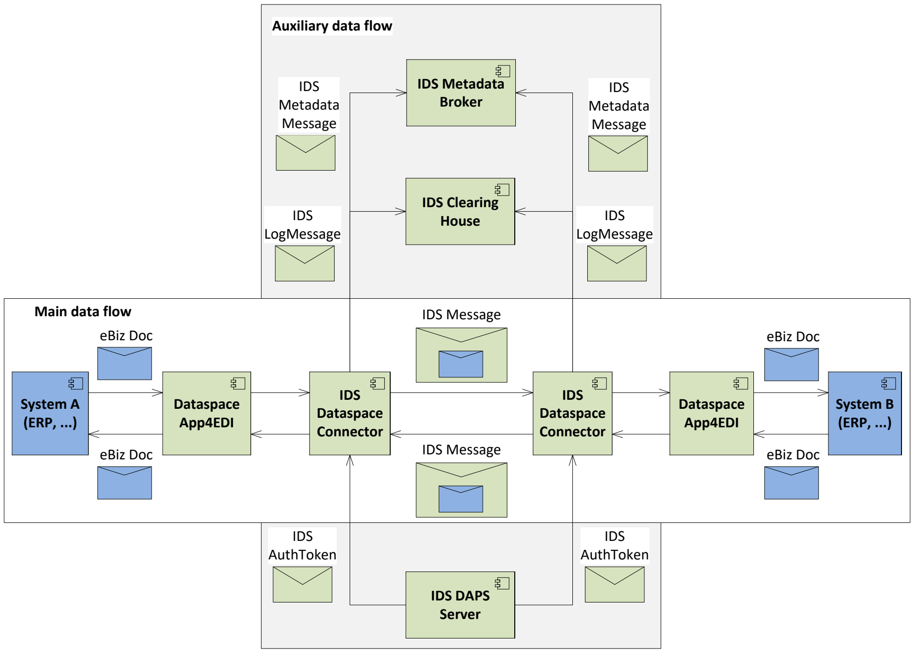

Fig. 2. Prototype Components and Data Flow

The prototype components and the data flow are presented in Fig. 2. It is intended that this architecture and components provide the full scope for performing production orders and checking the availability status from an industrial organization to its subcontractors.

The architecture assumes that a System A (e.g., Enterprise Resource Planning (ERP)) uses the eBiz[7] document type, and pretends to share its documents with a System B, through a DataspaceApp4EDI app. This application shares the document with the IDS Connector, which shares it with the other system connector and with the DataspaceApp4EDI of System B. This process is also performed in the reverse direction, from System B to System A. The auxiliary data flow comprises three IDS Components: IDS Metadata Broker, IDS Clearing House, and IDS DAPS Server. The DAPS Server and the IDS Clearing House are called every time the connectors communicate. The first is used to validate the connector's identity, and the latter to log messages to, if necessary, serve as an auditing entity. Finally, the IDS Metadata Broker is a catalogue of available IDS participants and components. Furthermore, the DataspaceApp4EDI serves as a bridge between the ERP and the IDS Connectors, with the responsibility of sending the eBiz files to the IDS Connector or the ERP.

The implementation featured three IDS Connectors, one Producer and two subcontractors connectors (i.e., Subcontracted-A and Subcontracted-B). Furthermore, the prototype was implemented using three machines running Ubuntu 20.04 LTS to test the DAPS interaction with the connectors. One virtual machine contains the Producer, the other the Subcontracted-A and Subcontracted-B, and another the DAPS, CA, Clearing House, and Metadata Broker.

4.2 Components Configuration

To communicate with the DAPS, the connectors need valid certificates. For that, a CA was implemented to create certificates for the connectors and components (i.e., Metadata Broker and Clearing House). In order to carry out tests, the Fraunhofer AISEC[8] *Omejdn* [19], a minimal but extensible OAuth 2.0/OpenID connect server, was used. The following procedures were executed:

1. modify the file concerning the *Omejdn* configuration,
2. update the docker environment variables file to use the DAPS with HTTPS and not in localhost,
3. modify the configuration file concerning the customers, and
4. add a TLS certificate from a trusted CA to use the DAPS with HTTPS.

For the initial DAPS configuration, it was necessary to update the protocol, environment, domain, TLS key, and certificate. Then, the *Omejdn* configuration required changes to guarantee consistency with the docker environment.

The implemented prototype used a sample CA made available by the International Data Spaces Association (IDSA), used to create trusted certificates

[7] `https://ebiz-tcf.eu/`

[8] `https://www.aisec.fraunhofer.de/en.html`

and guarantee that they have a valid hierarchy, which is necessary for the architecture. The certificates were created and the connectors and components were registered on the DAPS server. For that, each X.509 certificate created by the CA was added to the "/keys" directory of the DAPS server. Once the connectors and components were registered, they were configured as clients in the DAPS. Listing 1.1 presents a client configuration with its *id*, *name*, *scope*, *attributes* and *token endpoint authentication method*. Finally, the X.509 certificates on directory "/keys" were copied onto "/keys/client", with the name being the client id encoded to serve as the verification key.

Listing 1.1. clients.yml

```
- client_id: 12:05:B7:BB:F3:EA:DE:40:AA:AE:2E:D0:94:8F:FA:94:32:7D:54:1C
    :keyid:27:A8:D6:69:E6:25:47:BA:09:8D:98:E5:DF:79:3F:09:89:F4:4D:83
  client_name: subcontracted-A
  grant_types:
  - client_credentials
  token_endpoint_auth_method: private_key_jwt
  scope:
  - idsc:IDS_CONNECTOR_ATTRIBUTES_ALL
  attributes:
  - key: idsc
    value: IDS_CONNECTOR_ATTRIBUTES_ALL
  - key: referringConnector
    value: http://subcontracted_A.demo
  (...)
```

The keys and X.509 certificates were created and sent to the connectors. On the connector's machine, both files were used to create a *p12* file that was inserted into the connector configuration directory. Finally, its docker-composes were modified to use the instantiated DAPS instead of the default Fraunhofer one.

The Clearing House was also modified to use the new DAPS certificates and configuration, which consisted of sending the X.509 certificate and key to the component as well as the files to create a *p12* certificate inserted on the component bind mounts. As the DAPS is running HTTPS, its TLS certificate was sent to the Clearing House and moved to the directory "/docker" to be inserted into the trusted certificates folder of the operative system inside the docker container. Next, the container configuration files (i.e., *Rocket.toml*) were updated to redirect to the new DAPS instead of the Fraunhofer DAPS. Finally, the Clearing House connector was updated to also redirect to the new DAPS.

The Metadata Broker was updated to utilize the DAPS. Its docker-compose was edited to redirect to the new DAPS, and the certificates created by the CA were converted to the correct format and inserted into the proper directories. Next, the repository *application.properties* file was revised to redirect to the new DAPS and to include its URL on the trusted hosts. Finally, the DAPS TLS certificate was inserted into the docker files directory, guaranteeing that the new, untrusted certificate is inserted into the system folder when the component is built.

4.3 Communication testing

After configuring all components to use the DAPS instance, the interactions were tested. All communications between the IDS participants use the DAPS to validate their identity and thus, any request made by or to the connectors, the Clearing House, or the Broker involves the DAPS. To test the connectors, Clearing House, and DAPS interaction, the connectors started a contract agreement process. However, to test the Broker and DAPS communication, it is necessary a request by the connectors.

The Provider and Subcontracted-A connectors and the Clearing House were used to test the Connector, Clearing House, and DAPS interaction. The process is repeated by each component, i.e. although only involving the Producer and Subcontracted-A, the Clearing House is also performing the same steps to validate the connector's identity.

The contract agreement process starts with the subcontracted-A connector communicating with a connector provider. To do that, it needs to request a DAT to the DAPS to present to the connector provider. Thus, as a first step, the subcontracted automatically creates the JSON Web Token (JWT), which contains the header, payload, and signature. The signature is created with the subcontracted's private key, and the payload contains the fields described below:

- *aud*: token audience, which can be identified as the DAPS URL in this case.
- *exp*: JWT expiration date.
- *iat*: timestamp of when the JWT has been issued.
- *nbf*: "valid not before".
- *iss*: the component which created and signed the JWT, in this case, is the subcontracted connector.
- *sub*: the combined entry of the Subject Key Identifier (SKI) and Authority Key Identifier (AKI) of the intelligent DATA solutions (iDATAs) connectors X.509 certificate.

With the JWT created, the subcontracted connector is authenticated by presenting the JWT to the DAPS. The DAPS then receives the request from the connector and, based on it, assigns the DAT or not, by identifying whether the requesting connector is valid from the configured certificate. Listing 1.2 shows the encoded and decoded DAT.

Listing 1.2. DAT Token

```
[*] Dynamic Attribute Token:
{"access_token":"eyJ0eXAiOiJhdCtqd3QiLCJraWQiOiI2MGJlZmYxYWQ2N(...)",
"expires_in":3600,"token_type":"bearer","scope":"idsc:
    IDS_CONNECTOR_ATTRIBUTES_ALL"}
[*] DAT - Decoded:
{
  "typ": "at+jwt", "alg": "RS256",
  "kid": "60
      beff1ad662e38fd8996639286e3c24e2b366e52f87d88251b854096ef78c39"
}
{
  "scope": "idsc:IDS_CONNECTOR_ATTRIBUTES_ALL",
  "aud": [ "idsc:IDS_CONNECTORS_ALL" ],
  "iss": "https://vcese19.inesctec.pt/auth",
  "sub": "12:05:B7:BB:F3:EA:DE:40:AA:AE:2E:D0:94:8F:FA:94:32:7D:54:1C:
      keyid:27:A8:D6:69:E6:25:47:BA:098D:98:E5:DF:79:3F:09:89:F4:4D:83",
  "nbf": (...), "iat": (...), "jti": "b34ae7(...)", "exp": (...),
  "client_id": "12:05:B7:BB:F3:EA:DE:40:AA:AE:2E:D0:94:8F:FA:94:32:7D
      :54:1C:keyid:27:A8:D6:69:E6:25:47:BA:09:8D:98:E5:DF:79:3F:09:89:F4
      :4D:83",
  "securityProfile": "idsc:BASE_SECURITY_PROFILE",
  "referringConnector": "http://subcontracted.demo",
  "@type": "ids:DatPayload", "@context": (...),"transportCertsSha256":
      (...)
}
```

After receiving the DAT, the subcontracted-A connector shares it with the Provider connector. The provider analyzes the DAT fields, verifies if it is valid, and gives access to its services. The DAPS signs the received DAT and the client can verify this signature by retrieving the DAPS's public key(s) using a public endpoint (identified by the *iss* field in Listing 1.2). This process only shows whether the DAPS successfully authenticated the component. The exact process occurs between the Clearing House, the DAPS, and the connector that logs the message to the first component.

Regarding the Metadata Broker interaction with the DAPS, a connector is used to request the Broker. For this purpose, the description endpoint on the producer connector was used to receive the Broker's self-description.

5 Discussion

The transition of the textile and clothing industry to an Industry 4.0 environment, implies exchanging data between companies while assuring its authenticity, confidentiality, and integrity. The architecture defined had requirements of the STVgoDigital project, however, the prototype was implemented to provide the full scope for performing production orders and checking the availability status from an industrial organization to its subcontractors, as required in the textile and clothing industry sector. Thus, this architecture can be applied to other use cases within the textile and clothing industry, or other activity sectors where the requirements are similar.

The prototype is based in IDS which enables secure communications between trusted participants. The IDS Identity Provider and the IDS Connectors were implemented, which are the components responsible for guaranteeing safe data exchange. In this implementation, only trusted entities can be registered in the DAPS, which is responsible for managing the participants' dynamic attributes and a specific CA is responsible for managing the participants' digital certificates.

IDS is still a recent standard and future efforts should be dedicated to implementing this type of approach in other use cases. In order to foster these implementations, it is important to provide complete and up-to-date IDS documentation.

6 Conclusions

In order to operate their businesses, organizations from multiple activity sectors should manage their data and suppliers and manufacturers may benefit from the implementation of Industry 4.0 technical principles. Data exchange between corporations operating in the same or distinct activity sectors is required while upholding data sovereignty. Adequate standards and recommendations must be selected based on the specific requirements for these interactions, and the implementations should follow the security-by-design principles.

This paper presents the implementation of a prototype based on the IDS virtual data spaces to ensure secure communications between participants in the textile and clothing activity sector. The IDS-RAM is used as a base reference model since it meets the given requirements and aids data sharing securely while assuring data sovereignty for peers and clusters of peers. With the IDS virtual data space, the data exchange and linkage can be preserved in a reliable business ecosystem while facilitating cross-company business processes. This prototype implementation can be applied and linked with the required modifications to other textile and clothing corporations or other activity sectors, as it is valuable as a base model to encourage fruitful collaboration between all participants.

Acknowledgments

This study was developed in the context of the Master in Cybersecurity Program at the Instituto Politécnico de Viana do Castelo, Portugal.

This work was funded by European Regional Development Fund (ERDF) through the COMPETE2020 Programme, within the STVgoDigital project (POCI-01-0247-FEDER-046086).

References

[1] *STVgoDigital*. URL: http://www.stvgodigital.pt/ (visited on 01/30/2021).

[2] Ghaidaa Shaabany and Reiner Anderl. "Security by Design as an Approach to Design a Secure Industry 4.0-Capable Machine Enabling Online-Trading of Technology Data". In: *2018 International Conference on System Science and Engineering (ICSSE)*. 2018, pp. 1–5. DOI: 10.1109/ICSSE.2018.8520195.

[3] *The Internet of Things and Services Graphics © Bosch Rexroth AG*. URL: https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf (visited on 01/29/2021).

[4] Amr I. Elkhawas and Marianne A. Azer. "Security Perspective in RAMI 4.0". In: *2018 13th International Conference on Computer Engineering and Systems (ICCES)*. 2018, pp. 151–156. DOI: 10.1109/ICCES.2018.8639235.

[5] Holger Flatt et al. "Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements". In: *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. 2016, pp. 1–4. DOI: 10.1109/ETFA.2016.7733634.

[6] Silia Maksuti et al. "Towards flexible and secure end-to-end communication in industry 4.0". In: *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*. 2017, pp. 883–888. DOI: 10.1109/INDIN.2017.8104888.

[7] *GAIA-X: Technical Architecture.* URL: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=5 (visited on 03/03/2021).

[8] *International Data Spaces (IDS) makes it safe and easy to exchange data — TNO.* URL: https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/international-data-spaces-ids/ (visited on 01/29/2021).

[9] *Industrial Data Space - the secure data exchange model for industrial IoT.* URL: https://www.i-scoop.eu/industry-4-0/industrial-data-space/ (visited on 01/29/2021).

[10] Michael Nast et al. "Work-in-Progress: Towards an International Data Spaces Connector for the Internet of Things". In: *2020 16th IEEE International Conference on Factory Communication Systems (WFCS)*. 2020, pp. 1–4. DOI: 10.1109/WFCS47810.2020.9114503.

[11] Haydar Qarawlus et al. "Sovereign Data Exchange in Cloud-Connected IoT using International Data Spaces". In: *2021 IEEE Cloud Summit (Cloud Summit)*. 2021, pp. 13–18. DOI: 10.1109/IEEECloudSummit52029.2021.00010.

[12] Michael Nast et al. "Work-in-Progress: Towards an International Data Spaces Connector for the Internet of Things". In: *2020 16th IEEE International Conference on Factory Communication Systems (WFCS)*. 2020, pp. 1–4. DOI: 10.1109/WFCS47810.2020.9114503.

[13] Miguel A. Iñigo et al. "Towards Standardized Manufacturing as a Service through Asset Administration Shell and International Data Spaces Connectors". In: *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*. 2022, pp. 1–6. DOI: 10.1109/IECON49645.2022.9968592.

[14] Friedrich Volz, Ljiljana Stojanovic, and Robin Lamberti. "An Industrial Marketplace - the Smart Factory Web Approach and Integration of the International Data Space". In: *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*. Vol. 1. 2019, pp. 714–720. DOI: 10.1109/INDIN41052.2019.8972061.

[15] Danniar Reza Firdausy et al. "Towards a Reference Enterprise Architecture to enforce Digital Sovereignty in International Data Spaces". In: *2022 IEEE 24th Conference on Business Informatics (CBI)*. Vol. 01. 2022, pp. 117–125. DOI: 10.1109/CBI54897.2022.00020.

[16] *Reference Architecture Model.* URL: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf (visited on 01/30/2021).

[17] *Usage Control in the International Data Spaces (Position Paper).* URL: https://internationaldataspaces.org//wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3..pdf (visited on 08/18/2022).

[18] *Home - Dataspace Connector.* URL: https://github.com/International-Data-Spaces-Association/DataspaceConnector (visited on 12/02/2021).

[19] *Fraunhofer-AISEC/omejdn-server.* URL: https://github.com/Fraunhofer-AISEC/omejdn-server (visited on 12/10/2021).