ZDMP Blog

Data Privacy in Industry 4.0

By Tim Dellas. Ascora GmbH

Some questions for you

- How secure is your Business Data?
- Can trade secrets be reconstructed when analysing your companies' private data?
- Do you trust Microsoft, Apple and Amazon to keep your data private?
- Would you trust any new company or innovator to keep your data private?

Motivation

Imagine a world, where access to Industry 4.0 software platforms is a necessity to stay competitive. Industry 4.0 works with your company's data, which might well contain business "secrets", through which other companies or countries might be able to steal your innovations. Therefore, all EU platforms have to use the highest security standards and comply with EU data privacy laws. But is this enough to safeguard your data, and thereby, your business?

For every business activity, especially those with multiple partners, data privacy is a hard challenge to tackle. The European Union is pioneering data privacy laws, giving guidance and explicit rules, and considerations to be taken, but still the concrete implementation of a complex project, such as the Industry 4.0 platform ZDMP, has to take into account that for its customers, it's dealing with their most precious resource: Knowledge. Even raw data – in the wrong hands – can be used to reverse-engineer trade secrets.

This blog post is the latest in the Security & Privacy post series for ZDMP, which already addressed: Why Cybersecurity Risk Assessment Matters in Industry 4.0, Securely Installing Third-Party Apps for Industry 4.0, Secure Authentication and Authorization and Secure Communication Channels in Industry 4.0, as well as posts concerned with Data Privacy such as Ethics Related to the Use of Data and AI Technologies and Legal Issues in Data Exchange, where we've already talked about Trade Secrets, Data Privacy and what ZDMP will do in this regard. This post will expand in this direction.

Multiple possibilities to keep data private are evaluated in this post:

- Data Management Plan, Rules and Regulations
- Security of transmission channels and data storage; as a basis for Data Privacy
- Physical confinement of data to the Intranet; so data can be used without transferring it off-site
- Component-agnostic data-item-based data access model

Data Management Plan, Rules and Regulations

The first step to Data Privacy when building a new distributed system is looking at the recommendations and regulations put in place by the European Commission. This covers GDPR compliance and need to put into place concrete processes for user companies, in terms of data transaction contracts to be used, continuous monitoring of data claims (which data is claimed by every particular component, what is the purpose of data use), use and deletion of data, intellectual property management. ZDMP has internally worked on activities related to Regulation and Trustworthy system and the ZDMP exploitation company, i4FS will regulate this aspect via their contractual agreements and information.

Security of transmission channels and data storage

In many blog posts ZDMP covered that guaranteeing the security of transmission channels through appropriate encryption, use of appropriate Standards (what the consortium handled in D4.6: Standardisation Plan and Status Report) and of course by defining the architecture, Functional and Technical Specifications of the single Security-relevant components in ZDMP. Further information can also be found in blogs about Cybersecurity Risk Assessment and Secure Communication Channels, as well as security standards in the context of Secure Authentication and Authorisation and, rather specialized topic, of Securely Installing 3rd Party Platform Apps.

In summary, ZDMP uses fully secure and encrypted Data Transport Layers, a standards-based identify management system and standards-conforming authentication, and authorisation system bringing into play all useful security features, such as two-factor authentication and using firewall technology where it is useful. It makes use of virus checking for 3rd party zApps, human reviews of 3rd party applications and also uses access permissions for zApps, which

are known from apps on smartphones. Additionally, manufacturing companies' systems and infrastructure can be modelled in a special tool to check for security issues, to ensure the infrastructure is as secure as possible.

Physical confinement of data to the Intranet

One straightforward way to guarantee data privacy is to not to connect to the Cloud at all! ZDMP will provide this feature by making the whole platform federated and locally hostable – even the 3rd party zApps can connect to the local instances of the ZDMP cluster after an initial configuration of the User Management system and the Platform infrastructure. A local installation of course may have additional costs associated with it eg server hosting, additional software etc and might be more expensive solution in terms of total-cost-of-ownership vs i4Fs for example, but still this model can guarantee that companies' data remain in their control, on-site. This means, if your management does not trust external parties at all – which might be a reasonable view in respect to trade secrets – your company can use the platform without data leaving your servers.

Component-agnostic data-item-based data access model

Technical models that ensure data privacy even in the Cloud are complex to conceptualise and implement. The groundwork for this was created by ZDMP by deciding for the OpenID and OAuth2.0 Standards and using a User Management model, where groups and privileges can be adapted in a fine-grained way. To guarantee data privacy, the permissions have to be managed for each data item, whilst the data item travels through components. Moreover, the data itself would have to be encrypted by default and would have to be decrypted by each single component using the access token of the current user. To the best knowledge of the ZDMP consortium, such a system does not exist yet, and, as ZDMP is not a project for developing novel security systems, ZDMP has to approximate its solution as closely as possible to this ideal world that might well exist in the future.

While a full encryption of all data would be the best Data Privacy feature, as detailed in the ZDMP-provided paper "Evolution of Industry 4.0 Platforms within H2020 Projects" (IESA 2020), full encryption, if it is not fully homomorphous, will hamper the searchability and therefore the use of data and the utility of data itself. Until this technology is available, there is no better solution than to keep permissions' records for every single document or data item, which is the data privacy mechanism adopted by big data providers such as Microsoft, Apple and Google. As Open-Source technology in this field is rare, especially when it comes to data privacy of database entries (vs. document management systems, where there are solutions available), ZDMP's Secure Data Storage task force is currently investigating Open-Source databases. Solutions need to support OAuth2.0 and OpenID powered users and user-groups in order to enable federated components to access documents and data for the current user agent interacting with the component. Also, when accessing a resource with an API request (so even without direct interaction of a user), the accessing software has to provide the user's ID that the software representation in its interaction, so the generated data will be sealed / audited for the user or the user's permission group.

What will ZDMP achieve

ZDMP aspires to respect and implement all regulations and suggestions by the European Union in regard to data privacy and also follow (and even help to create new) standards in the field. Also, ZDMP creates a federated, completely self-hostable platform for maximum data privacy as a premium privacy feature. In addition, ZDMP follows the OpenID protocol for authentication, implements context-based authentication together with multi-factor authentication and use the OAuth2 and Role-based Access Control (RBAC), as well as Attribute-based Access Control (ABAC) mechanisms to manage access to protected resources. The project also has a data management plan for partners, and as a whole, which is regularly updated

ZDMP Links

• **Architecture Component(s)**	Cloud Storage, Platform
• **Work Package**	WP6 – ZDMP Platform Building
• **Tasks**	T6.2 – Secure Business Cloud T6.4 – Platform Integration and Federation