Fraunhofer

IESE

MYDATA
CONTROL TECHNOLOGIES

The challenge

The exchange of data presents companies with great challenges: On the one hand, legal requirements must be fulfilled, for example requirements from the European General Data Protection Regulation (GDPR) such as self-determination and transparency. On the other hand, data exchange with business partners always becomes a risk whenever it involves sensitive, personal, or business-critical data. Granting access to one's data without exercising control entails great risk. However, it would be counterproductive and would diminish the company's competitiveness to forego exchange entirely. This is why companies need to find a balance in order to take advantage of the opportunities without disregarding the risks.

Typical issues

■ How to control and manage data interfaces at runtime?

■ How to effectively filter or mask sensitive, personal, or business-critical information in data flows at runtime?

■ How to ensure uniform implementation of data sovereignty?

■ How to react quickly to new privacy challenges without having to modify the software?

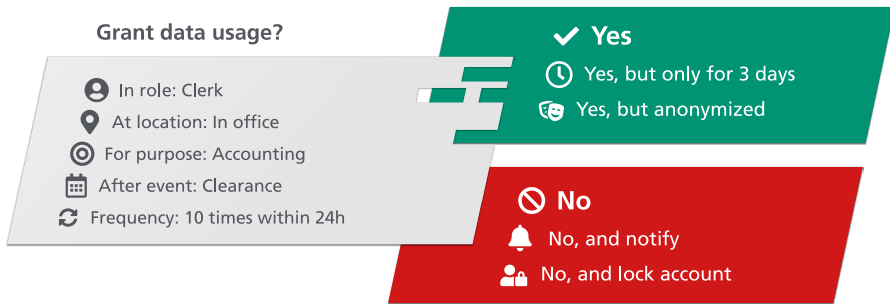■ How to anonymize or encrypt data flows without major effort?

The solution

MYDATA Control Technologies (MYDATA) enables companies to strike a smart balance in data transfer: They can filter or mask their data in accordance with legal requirements and company regulations before passing it on.

MYDATA is a technical implementation of data sovereignty that represents an essential component for informational self-determination. It is based on the IND²UCE framework for data usage control devel-

oped at Fraunhofer IESE. MYDATA implements data sovereignty by interfering in security-relevant data flows. This enables fine-grained masking and filtering of data flows at interfaces (APIs) in order to make these anonymous, for example. Compared to traditional access control systems, MYDATA can enforce partial filering and masking of data, context- and situation-dependent restrictions, as well as limitations regarding the usage purpose. Compliance with data sovereignty through changes in the data flows is controlled by a set of policies.

Grant data usage?

- In role: Clerk
- At location: In office
- For purpose: Accounting
- After event: Clearance
- Frequency: 10 times within 24h

✔ **Yes**
- Yes, but only for 3 days
- Yes, but anonymized

🚫 **No**
- No, and notify
- No, and lock account

Context-based usage rules with MYDATA

The benefits of MYDATA Control Technologies

- Central services for the management and control of data flows at runtime

- Flexible set of policies for mapping data sovereignty requirements

- Uniform technical enforcement of data sovereignty requirements

- Adaptive behavior due to inclusion of contextual information

- Easy integration due to open-source SDK and detailed tutorials

- Numerous extension possibilities due to plugin concept

Application example 1: Data exchange between companies (B2B)

Many companies already recognize the enormous potential in the collection, analysis, and exchange of a wide variety of data. However, they also see high risk when it comes to exchanging sensitive data with business partners. If, for example, a supplier wants to notify a company of an imminent delivery bottleneck, this information should not be published or disseminated in an uncontrolled manner. In such a case, MYDATA can ensure that usage of this data is limited in terms of time and that only an authorized group of people can use this data. When exchanging data between companies, there are many other requirements regarding data sovereignty that MYDATA helps to fulfill.

Application example 2: Data release in banking (C2B2B)

The EU Payment Service Directive (PSD2) regulates, among other things, participation in the payment industry by non-banks. External companies can get access to transaction and customer data in order to offer the bank customer added value. PSD2 interfaces with MYDATA offer bank customers self-determination when their data is used by third parties. The bank customers decide for themselves which transaction data will be released to external companies. For this purpose, the data can be filtered and masked with MYDATA. To assess a customer's creditworthiness, monthly income and expenses are relevant, but the bank customer might not want to disclose all transaction details. Here, MYDATA creates more trust by strengthening the data sovereignty of bank customers.

Application example 3: Digitalized rural areas (C2C)

Even in rural areas, digitalization is making great progress. The Digital Villages Platform (www.digitale-doerfer.de) of Fraunhofer IESE enables municipalities and local authorities to offer digital services to their citizens. For example, there is a delivery service: Citizens can ask others to deliver products from regional shops to their door. By default, such requests are publicly visible. Here, MYDATA protects the privacy of the citizens. Further details about the delivery, such as the exact delivery address, are only shown to the person making the delivery. If the person who requested the delivery is not home, he or she can specify a secret drop-off location, which the person making the delivery will only see on their smartphone when they are located in the vicinity of the delivery location. For this purpose, MYDATA uses contextual information, such as the location of the person making the delivery, to control data usage.

Application example 4: Data loss prevention in own company (B2x)

The – mostly unintentional – disclosure of sensitive information is a constant threat for companies. This is often caused by the carelessness of employees and not by hackers or malicious intent. An employee sends an email to external recipients and has inadvertently attached a confidential, internal Office document. In order to prevent such scenorios, the MYDATA Control Office plugins offer suitable solutions. Documents in a wide variety of formats (incl. Word, Excel, PowerPoint, PDF) can be classified according to their level of confidentiality and their usage can be controlled. For example, when attachments are mailed, MYDATA monitors that internal documents are only mailed to external recipients after explicit confirmation. Confidential documents may only be sent after being encrypted. MYDATA thereby prevents undesired data leaks.

Our Technology

MYDATA Control Technologies consists of three core functions:

- **MYDATA Control Enforcement**: MYDATA offers control points for the enforcement of usage policies, which can be easily integrated into target systems. These can filter and mask information at data interfaces. In addition, MYDATA offers the possibility to execute actions by using additional components, such as email notification. The functionality of the control points and the execution of actions can be extended through plugins.

- **MYDATA Control Policies**: New policies on data usage can be created at runtime. Settings include, among others, time- and frequency-based usage ("Data may only be used 5 times within one day"), situation-based usage ("Sensitive data may not be viewed on business trips"), and masked usage ("For PSD2 service providers, the middle 12 digits of the IBAN are replaced by an X").

- **MYDATA Control Management**: MYDATA combines the management of data sovereignty requirements and technical components in one central management console.

The modular and component-based structure of MYDATA permits easy and scalable integration into existing systems. The plugin concept offers a wide variety of extension options, including connection to other systems (e.g., to directory services). To this end, a Software Development Kit with comprehensive documenta-
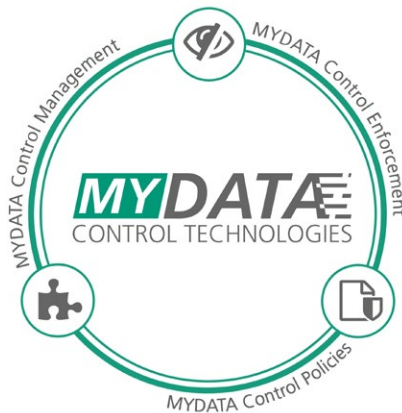
Core functions of MYDATA

tion provides suitable support for developers. MYDATA can be extended with three types of plugins:

- **Data modification**: MYDATA controls and modifies data flows based on the active policies. Example policy: "Remove all customer addresses before passing data on to third parties."

- **Action execution**: MYDATA executes (compensating) actions based on the active set of policies. Example policy: "If someone accesses my data, notify me via email."

- **Information resolution**: MYDATA integrates various kinds of information sources, such as geodata or directory information. Example policy: "Only allow access if the user has the role of Administrator and is located on the premises of the company."

Our Services

With MYDATA Control Technologies, we are providing an effective software solution for achieving data sovereignty. We will also gladly support you with individual services custom-tailored to your needs:

- **Potential Analysis**: Do you want to find out how MYDATA can be used to protect your data? In a workshop we will work out usage scenarios for MYDATA in your company together with you.

- **Piloting**: Do you want to test MYDATA Control Technologies in your organization? Our developers will be happy to support you in implementing a proof of concept in the context of your company.

- **Developer support**: Do you want support in integrating MYDATA into your system, in developing your own plugins, or in specifying usage policies for your use cases? Our experts will be happy to support you in solving your individual challenges.

Contact at Fraunhofer IESE

Denis Feth
Department Head
Security Engineering
denis.feth@iese.fraunhofer.de
Phone +49 631 6800-2157
www.iese.fraunhofer.de

Fraunhofer Institute for Experimental Software Engineering IESE

Fraunhofer-Platz 1
67663 Kaiserslautern
Germany

Further information about MYDATA Control Technologies can be found at:
https://www.mydata-control.de

Fraunhofer IESE

The Fraunhofer Institute for Experimental Software Engineering IESE in Kaiserslautern has been one of the world's leading research institutes in the area of software and systems engineering for more than 20 years. Its researchers have contributed their expertise in the areas of Processes, Architecture, Security, Safety, Requirements Engineering, and User Experience in more than 1,200 projects. The institute is working on innovative topics related to digital ecosystems, such as Industrie 4.0, Big Data, and Cyber-Security. It is a technology and innovation partner for the digital transformation in the areas of Autonomous & Cyber-Physical Systems and Digital Services, and its research focuses on the interaction between embedded systems and information systems in digital ecosystems.

Fraunhofer IESE is one of 72 institutes and research units of the Fraunhofer-Gesellschaft. Together they have a major impact on shaping applied research in Europe and contribute to Germany's competitiveness in international markets.