Fraunhofer
IESE

FRAUNHOFER INSTITUTE FOR EXPERIMENTAL
SOFTWARE ENGINEERING IESE

IND²UCE – INTEGRATED DISTRIBUTED DATA USAGE CONTROL ENFORCEMENT

Integrated Distributed Data Usage Control Enforcement (IND²UCE)

In modern IT applications and services, large amounts of business-critical and personalized data are processed and exchanged continuously. This may even happen unintentionally or unnoticed. It is therefore of crucial importance to both companies and individual users to be able to control the usage (including the dissemination) of sensitive or secret data in order to prevent any misuse right from the start. The lack of suitable security measures in this area can lead to identity theft, disclosure of secret official documents, or loss of reputation due to the violation of customer privacy.

Data usage control, an extension of classic access control, offers an effective and flexible approach for this situation. It allows specifying and enforcing guidelines for regulating the usage of data after initial access was granted.

Data usage control enables the establishment of security policies of any degree of granularity that also cover time-related and frequency-based aspects. Granularity can range from strict separation of domains to protective mechanisms regulating the usage of concrete data. This allows guaranteeing comprehensive protection of data; at the same time, more rigorous security measures can be established for selected secret data. In this context, we specifically look at the following attack models:

- Unintentional passing or usage of sensitive data.
- Intentional misuse in the sense of data sharing or usage by attackers without administrator rights.

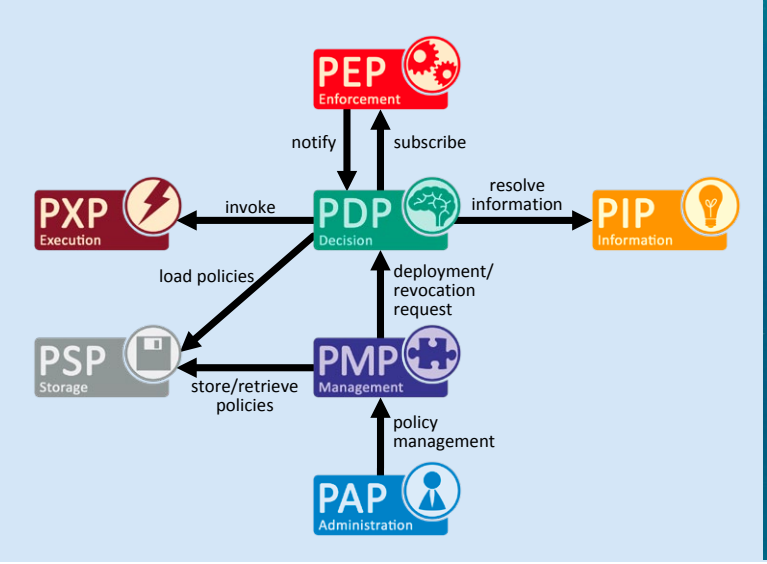
IND²UCE Security in Your Business!

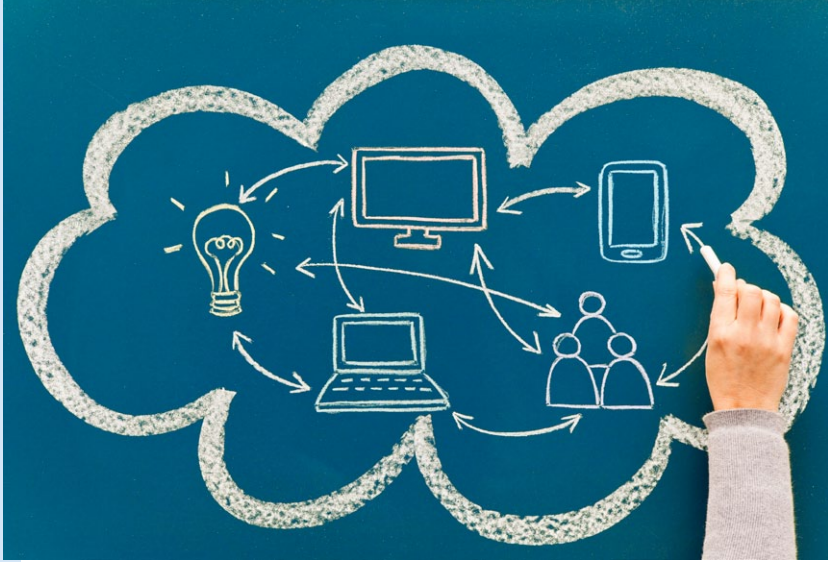
Distributed data usage control allows controlling the dissemination and usage of your data beyond the initial access. Data usage control extends established access control and digital right management solutions and can offer your organization added value in the area of data security, thus addressing many of your daily data privacy and business challenges.

There are many examples that illustrate the security gained by employing data usage control in your organization:

- When mobile devices are integrated into everyday business, it should be possible to use them for both business and private use, but personal and business data should not be mixed or disseminated inadvertently.
- Connecting various services in a company context is standard practice in business contexts today. Data usage control ensures that data do not inadvertently cross system boundaries let alone company borders.
- A continuing trend in the interconnection of services is cloud computing. In cloud environments, data usage control also offers a proven way to maintain control over the dissemination and usage of your data.
- Novel types of business models lead to increased interconnections between businesses and services. Data usage control offers efficient protective mechanisms for maintaining cross-company control over secret data in such a heterogeneous and confusing landscape.

Data usage control represents an adequate instrument for mastering these and similar problems. We will gladly provide you with more application examples to convince you of the benefits of our efficient solutions in the area of data usage control.





Protection across Abstraction Levels and Systems

Data are generally processed on several abstraction levels of a system. For example: Data on the application level can be multiplied by sending an email, while data on the operating system level can be multiplied by taking a screenshot. In order to protect sensitive data from undesired usage, data usage control must therefore be enforced on several levels of abstraction. To do so, we integrate our security components on all system levels necessary in order to achieve the best possible protection.

In addition to the protection of data within a system, Fraunhofer IESE is also performing research into data usage control in distributed company networks and in scenarios in which data are exchanged across company borders, and is developing cloud-based solutions as well.

Component-based Framework

The IND²UCE framework of Fraunhofer IESE comprises all components that are necessary to assure comprehensive data usage control in your company. It is based on common standards such as XACML, and its component-based structure allows achieving custom-tailored security for any usage area. Depending on the use case, new components can be seamlessly integrated into the existing IND²UCE framework.

The framework allows specifying security guidelines that can help to determine the legitimacy of security-relevant events (e.g., data operations). These security guidelines are based on the Obligation Specification Language (OSL), which permits the specification of security policies and future obligations.

Our Services

Support in the Development and Integration of Usage Control Solutions and Feasibility Evaluations

- Conceptual and technical support for the integration of data usage control components into applications and company networks
- Support in the development of customer-specific components on the basis of the IND²UCE framework
- Customer-specific adaptations and extensions of existing IND²UCE components to individual use cases

Data Usage Control on Mobile Devices

- Conceptual solution for data usage control on mobile devices
- Technical support for the integration of data usage control into mobile devices

Elicitation of Security Guidelines and Policies

- Identification of sensitive data
- Specification of organization-wide standard guidelines and policies
- Transfer of competencies in the area of policy specification
- Policy language for the specification of data usage control guidelines

Easy-to-Use Editors for the Specification of Security Guidelines and Policies

- Determination of the user group
- User-centered usability concepts for the development of policy editors

Context-Sensitive Enforcement of Security Guidelines and Policies

- Models for the aggregation of sensor values
- Context recognition on various levels of abstraction
- Context-sensitive activation of security guidelines and policies

Model-based Refinement of Security Guidelines and Policies based upon Business Processes

- Refinement of business processes on the implementation level
- Definition of security guidelines on the business process level
- Refinement of security guidelines on the implementation level

Support of the Software Development Process with Focus on Data Security and Data Usage Control

- Requirements analysis and elicitation
- Support in the design of a suitable software and security architecture

Contact

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

Institute Directors

Prof. Dr.-Ing.
Peter Liggesmeyer

Fraunhofer Institute for Experimental Software Engineering IESE

Software is a part of our lives. Embedded into everyday equipment, into living and working environments or modern means of transportation, countless processors and controllers make our lives simpler, safer, and more pleasant. We help organizations to develop software systems that are dependable in every aspect, and empirically validate the necessary processes, methods, and techniques, emphasizing engineering-style principles such as measurability and transparency.

Fraunhofer IESE in Kaiserslautern is one of the worldwide leading research institutes in the area of software and systems engineering methods. A major portion of the products offered by its customers is defined by software. These products range from automotive and transportation systems via automation and plant engineering, energy management, information systems, and health care to software systems for the public sector. The institute's software and systems engineering approaches are scalable, which makes Fraunhofer IESE a competent technology partner for organizations of any size from small companies to major corporations.

Under the leadership of Prof. Peter Liggesmeyer and Prof. Dieter Rombach, the contributions of Fraunhofer IESE have been a major boost to the emerging IT hub Kaiserslautern for more than twenty years. In the Fraunhofer Information and Communication Technology Group, the institute is cooperating with other Fraunhofer institutes to develop trend-setting key technologies for the future.

Fraunhofer IESE is one of 69 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.

2023-10