Fraunhofer

IESE

FRAUNHOFER INSTITUTE FOR EXPERIMENTAL SOFTWARE ENGINEERING IESE

DATA USAGE CONTROL
SHARE DATA, KEEP CONTROL!

DIGITAL TRANSFORMATION AND THE PROTECTION OF CUSTOMER DATA.

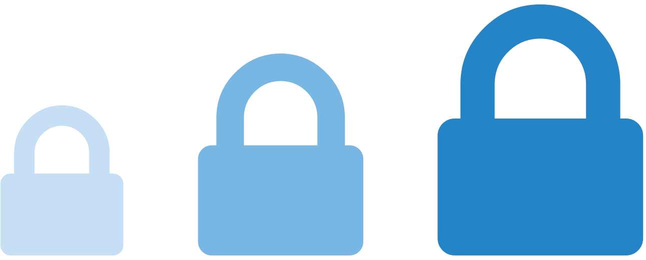
Today's business models are more and more data-driven. This means that they increasingly rely on the processing and exchange of data—especially customer data. However, both customers and legal authorities demand comprehensive protection of this data. The EU General Data Protection Regulation contains core principles that must be implemented (e.g., transparency, explicit consent, and purpose control). Infringements can be fined with up to 4 percent of the offender's yearly global turnover.

However, traditional security solutions are not aligned with today's data protection principles. Modern system landscapes are highly dynamic, heterogeneous, and largely interconnected. At the same time, many security concepts we apply today stem from the 1970s. They are neither powerful nor flexible enough to assure comprehensive data protection in the age of steadily advancing digital transformation. These solutions do not allow keeping control over data once access has been granted. Especially purpose control is a major issue, as it extremely hampers the involvement of third-party services, on which we all rely.

New concepts are needed in order to make use of customer data while protecting it effectively. The concept for mastering these numerous challenges is what we call *data usage control*.

Share Data, Keep Control

Typically, security solutions only regulate access to data. However, this is not enough to prevent future data misuse. After legitimate access has been granted, the subsequent use of the data has to be controlled, too, in order to ensure that it is only used for the intended purpose. To this end, access control has to be complemented with usage control.



Imagine, for example, that you are lending your car to a friend. Once you have given him the car keys, you have completely lost control over your car. If the car were to be usage-controlled, you could keep (at least some) control. For example, you could limit the maximum speed or the traveling distance. Of course, one challenge at this point is to strike the right balance between restriction and utility: While the speed limit can be actively enforced in our example, it does not make sense to stop the car immediately when the distance limit has been reached. However, you could at least be notified about this violation and track the car's position from that time on.

When compared to access control policies, usage control policies are much more expressive and powerful, and thus offer

greater flexibility. This has four major reasons: First, usage control policies contain restrictions that do not have to be enforced in the present, but rather in the future (e.g., data has to be deleted the latest 14 days after the initial use). Second, usage control decisions are not simply "yes" (i.e., grant access) or "no" (i.e., inhibit access). Instead, they are typically of the form "yes, but…" (e.g., usage is allowed, but only if person-related data is anonymized). Third, to make decisions based on usage, the purpose of use and the usage situation must be taken into account. For example, it needs to be identified whether a user wants to read a sensitive file in a safe or in an unsafe environment (e.g., in a secured office or on a public train). Finally, data has to be protected regardless of where it flows (e.g., server, desktop, mobile) and independent of its manifestation (e.g., file, email, clipboard).

Where We Are Now

Data usage control has been approached from a research perspective for over a decade. Theoretical foundations have been partially transferred into practice. Our policy language and policy evaluation are generic and formally verified. Technical feasibility has been shown in a variety of case studies performed together with industry.

IND²UCE provides a generic and highly scalable service that can be used out-of-the box for specifying, managing, and evaluating usage control policies. Additionally, an easy-to-use software development kit (SDK) supports developers in implementing usage control in their systems.

IND²UCE SECURITY

What Remains to Be Done

We need to build a network of interested researchers, developers, users, and legislation. Together, we should aim to standardize usage control concepts and technologies. Standardization is the key for assuring compatibility and encouraging further development in the field of data usage control.

Conclusion

Data security is more than just controlling access. Companies have to control the usage of data while also protecting their own and their customers' valuable data assets. Data protection is more than a service to their customers and to themselves: It is a legal obligation. Thus, using a data usage control solution is a necessity for companies that want to make it possible to protect data by controlling its usage.

With IND²UCE, we provide a powerful, flexible, and easy-to-use solution for implementing data usage control. Our team supports you in protecting your sensitive data by integrating IND²UCE into your applications and networks. If you want to learn more about data usage control and IND²UCE, please visit us at **www.ind2uce.de**, or contact us via **ind2uce@iese.fraunhofer.de**.

Contact

Christian Jung
Department Head
Security Engineering
christian.jung@iese.fraunhofer.de
Phone: +49 631 6800-2146

www.iese.fraunhofer.de

Fraunhofer Institute for Experimental Software Engineering IESE

Fraunhofer-Platz 1
67663 Kaiserslautern
Germany

Institute Directors

Prof. Dr.-Ing.
Peter Liggesmeyer
Prof. Dr. Dr. h. c.
Dieter Rombach

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.

2017-03