



IND²UCE – INTEGRATED DISTRIBUTED DATA USAGE CONTROL ENFORCEMENT





Integrated Distributed Data Usage Control Enforcement (IND²UCE)

In modernen IT-Anwendungen und -Diensten werden ständig große Mengen an geschäftskritischen und personenbezogenen Daten verarbeitet und ausgetauscht. Dies kann unter Umständen sowohl unabsichtlich als auch unbemerkt vonstattengehen. Daher ist es für das Unternehmen, aber auch für den einzelnen Anwender essenziell wichtig, die Nutzung (einschließlich der Verbreitung) von schützenswerten oder geheimen Daten kontrollieren zu können, um einen Missbrauch von Beginn an zu verhindern. Das Fehlen geeigneter Sicherheitsmaßnahmen kann an dieser Stelle einen Identitätsdiebstahl, die Veröffentlichung von geheimen dienstlichen Unterlagen oder einen durch die Verletzung der Privatsphäre von Kunden bedingten Reputationsverlust zur Folge haben.

Datennutzungskontrolle (engl. Data Usage Control), eine Erweiterung der klassischen Zugriffskontrolle, bietet hier einen effektiven und flexiblen Ansatz. Dieser erlaubt die Spezifikation und Durchsetzung von Richtlinien, welche die Verwendung von Daten nach dem initialen Zugriff regeln.

Es erlaubt beliebig feingranulare Sicherheitsrichtlinien, welche auch zeitliche und häufigkeitsbasierte Aspekte abdecken. Die Granularität kann hier von einer strikten Trennung von Domänen bis hin zu Schutzmechanismen reichen, welche die Nutzung konkreter Daten regeln. Somit kann ein flächendeckender Schutz von Daten garantiert werden und gleichzeitig lassen sich für ausgewählte geheime Dokumente schärfere Sicherheitsmaßnahmen etablieren. Dabei betrachten wir konkret folgende Angreifermodelle:

- Unbeabsichtigte Weitergabe oder Nutzung von sensiblen Daten
- Bewusster Missbrauch im Sinne der Datenweitergabe oder -nutzung von Angreifern ohne Administratorrechte

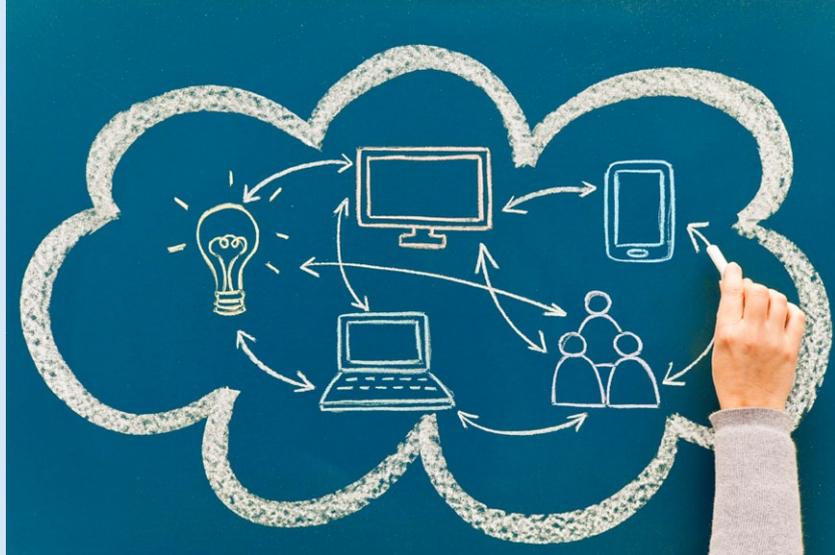
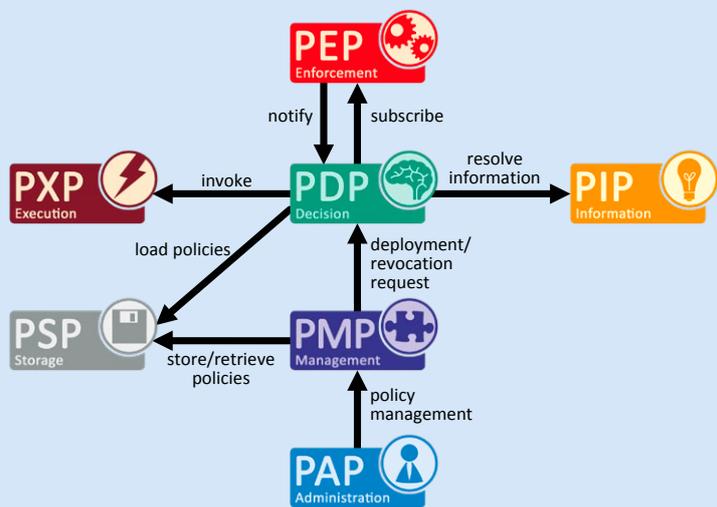
IND²UCE security in your business!

Verteilte Datennutzungskontrolle erlaubt es, die Verbreitung und Verwendung Ihrer Daten über den ersten Zugriff hinaus zu kontrollieren. Datennutzungskontrolle erweitert dabei etablierte Zugriffskontrolllösungen und kann Ihrem Unternehmen einen Mehrwert im Bereich der Datensicherheit bieten. Damit werden viele Ihrer täglichen Herausforderungen im Bereich des Datenschutzes adressiert.

Es gibt viele Beispiele, die den Sicherheitsgewinn beim Einsatz von Datennutzungskontrolle in Ihrem Unternehmen verdeutlichen:

- Bei der Einbindung mobiler Endgeräte in den Geschäftsalltag soll deren dienstliche aber auch private Nutzung ermöglicht werden, ohne dass persönliche und dienstliche Daten vermischt und unbeabsichtigt verteilt werden können.
- Die Vernetzung unterschiedlicher Dienste im Unternehmenskontext ist heutzutage die Norm. Datennutzungskontrolle sorgt dafür, dass keine Daten ungewollt Systemgrenzen oder gar Unternehmensgrenzen übertreten.
- Ein anhaltender Trend in der Vernetzung von Diensten ist Cloud Computing. Auch in Cloud-Umgebungen bietet die Datennutzungskontrolle ein probates Mittel, um die Herrschaft über die Verbreitung und Nutzung Ihrer Daten zu wahren.
- Neuartige Geschäftsmodelle führen zu einer höheren Vernetzung von Unternehmen und Diensten. Datennutzungskontrolle bietet wirksame Schutzmechanismen, um in einer solch heterogenen und unübersichtlichen Landschaft die unternehmensübergreifende Kontrolle über geheime Daten zu behalten.

Datennutzungskontrolle stellt ein adäquates Instrument dar, dieser und ähnlicher Probleme Herr zu werden. Wir überzeugen Sie gerne von den Vorzügen unserer Lösungen anhand weiterer Anwendungsbeispiele.



Abstraktionsebenen- und systemübergreifender Schutz

Daten werden in der Regel auf mehreren Abstraktionsebenen eines Systems verarbeitet. Beispielsweise können Daten auf Anwendungsebene durch das Senden einer E-Mail und auf Betriebssystemebene durch die Aufnahme eines Screenshots vervielfältigt werden. Um ein sensibles Datum vor ungewünschter Nutzung zu schützen, muss Datennutzungskontrolle folglich auf mehreren Abstraktionsebenen durchgesetzt werden. Dazu integrieren wir unsere Sicherheitskomponenten auf allen notwendigen Systemschichten, um den bestmöglichen Schutz zu erwirken.

Zusätzlich zum Schutz von Daten innerhalb eines Systems erforscht das Fraunhofer IESE insbesondere auch die Datennutzungskontrolle in verteilten Unternehmensnetzwerken und in Szenarien, bei denen Daten über Unternehmensgrenzen hinweg fließen.

Komponentenbasiertes Framework

Das IND²UCE Framework des Fraunhofer IESE umfasst alle Komponenten, welche zu einer umfassenden Datennutzungskontrolle in Ihrem Unternehmen führen. Es orientiert sich an gängigen Standards wie XACML und ermöglicht durch einen komponentenbasierten Aufbau maßgeschneiderte Sicherheit für jedes Einsatzgebiet. Je nach Anwendungsfall können neue Komponenten nahtlos in das bestehende IND²UCE Framework integriert werden.

Das Framework erlaubt die Spezifikation von Sicherheitsrichtlinien, mit deren Hilfe über die Legitimität von sicherheitsrelevanten Ereignissen (bspw. Dateioperationen) entschieden werden kann. Diese Sicherheitsrichtlinien basieren auf der Obligation Specification Language (OSL), welche die Spezifikation von Verbindlichkeiten erlaubt.

Unsere Leistungen

Unterstützung bei der Entwicklung und Integration von Nutzungskontrolllösungen

- Konzeptionelle und technische Unterstützung bei der Integration von Datennutzungskontrollkomponenten in Anwendungen und Unternehmensnetzwerken
- Unterstützung bei der Entwicklung von kundenspezifischen Komponenten auf Basis des IND²UCE Frameworks
- Kundenspezifische Anpassungen und Erweiterungen bestehender IND²UCE Komponenten auf den Anwendungsfall

Datennutzungskontrolle auf mobilen Endgeräten

- Konzepte für Datennutzungskontrolle auf mobilen Endgeräten
- Technische Unterstützung bei der Integration von Datennutzungskontrolle in mobile Endgeräte

Erhebung von Sicherheitsrichtlinien

- Spezifikation von unternehmensweiten Standardrichtlinien
- Vermittlung von Kompetenzen im Bereich der Richtlinien-spezifikation
- Bereitstellung einer Policy-Sprache zur Spezifikation von Richtlinien zur Datennutzungskontrolle

Einfach nutzbare Editoren zur Spezifikation von Sicherheitsrichtlinien

- Auf die jeweiligen Nutzer abgestimmte Nutzbarkeitskonzepte zur Entwicklung von Richtlinieneditoren

Kontextsensitive Durchsetzung von Sicherheitsrichtlinien

- Modelle zur Aggregation von Sensorwerten
- Kontexterkenntnis auf verschiedenen Abstraktionsebenen
- Kontextabhängige Aktivierung von Sicherheitsrichtlinien

Modellbasierte Verfeinerung von Sicherheitsrichtlinien anhand von Geschäftsprozessen

- Definition von Sicherheitsrichtlinien auf Geschäftsprozess-ebene
- Verfeinerung von Sicherheitsrichtlinien auf Implementierungsebene

Unterstützung im Softwareentwicklungsprozess mit Fokus auf Datensicherheit und Datennutzungskontrolle

- Anforderungsanalyse und -erfassung
- Unterstützung beim Entwurf einer geeigneten Software- und Sicherheitsarchitektur
- Testen von Datennutzungskontrollumsetzungen



Kontaktperson

Christian Jung
Abteilungsleiter
Security Engineering
christian.jung@iese.fraunhofer.de
Telefon: +49 631 6800-2146

www.iese.fraunhofer.de

Fraunhofer-Institut für Experimentelles Software Engineering IESE

Fraunhofer-Platz 1
67663 Kaiserslautern

Institutsleitung

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

Das Fraunhofer-Institut für Experimentelles Software Engineering IESE

Software ist Teil unseres Lebens. Eingebettet in Gebrauchsgegenstände, Wohn- und Arbeitsumgebungen oder moderne Transportmittel machen unzählige Prozessoren und Controller unseren Alltag einfacher, sicherer und angenehmer. Wir helfen Softwaresysteme zu entwickeln, auf die man sich in jeder Hinsicht verlassen kann. Die dazu erforderlichen Prozesse, Methoden und Techniken untermauern wir empirisch. Dabei legen wir Wert auf ingenieurwissenschaftliche Prinzipien wie Messbarkeit und Transparenz.

Das Fraunhofer IESE in Kaiserslautern gehört zu den weltweit führenden Forschungseinrichtungen auf dem Gebiet der Software- und Systementwicklungsmethoden. Die Produkte seiner Kooperationspartner werden wesentlich durch Software bestimmt. Die Spanne reicht von Automobil- und Transportsystemen über Automatisierung und Anlagenbau, Energiemanagement, Informationssysteme und Gesundheitswesen bis hin zu Softwaresystemen für den öffentlichen Sektor. Die Lösungen sind flexibel skalierbar. Damit ist das Institut der kompetente Technologiepartner für Firmen jeder Größe – vom Kleinunternehmen bis zum Großkonzern.

Unter der Leitung von Prof. Peter Liggesmeyer und Prof. Dieter Rombach trägt das Fraunhofer IESE seit über 20 Jahren maßgeblich zur Stärkung des aufstrebenden IT-Standorts Kaiserslautern bei. Im Fraunhofer-Verbund für Informations- und Kommunikationstechnik engagiert es sich gemeinsam mit weiteren Fraunhofer-Instituten für richtungsweisende Schlüsseltechnologien von morgen.

Das Fraunhofer IESE ist eines von 69 Instituten und Einrichtungen der Fraunhofer-Gesellschaft. Zusammen gestalten sie die angewandte Forschung in Europa wesentlich mit und tragen zur internationalen Wettbewerbsfähigkeit Deutschlands bei.