The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/1741-0398.htm

Usage control architecture options for data sovereignty in business ecosystems

Johannes Zrenner
Graduate School of Logistics, TU Dortmund University, Dortmund, Germany
Frederik Oliver Möller
Chair for Industrial Information Management, TU Dortmund University, Dortmund, Germany
Christian Jung and Andreas Eitel
Fraunhofer IESE, Kaiserslautern, Germany, and
Boris Otto
Chair for Industrial Information Management, TU Dortmund University, Dortmund, Germany and Fraunhofer ISST, Dortmund, Germany

Received 9 March 2018
Revised 9 February 2019
Accepted 26 February 2019

Abstract

Purpose – Current business challenges force companies to exchange critical and sensitive data. The data provider pays great attention to the usage of their data and wants to control it by policies. The purpose of this paper is to develop usage control architecture options to enable data sovereignty in business ecosystems.
Design/methodology/approach – The architecture options are developed following the design science research process. Based on requirements from an automotive use case, the authors develop architecture options. The different architecture options are demonstrated and evaluated based on the case study with practitioners from the automotive industry.
Findings – This paper introduces different architecture options for implementing usage control (UC). The proposed architecture options represent solutions for UC in business ecosystems. The comparison of the architecture options shows the respective advantages and disadvantages for data provider and data consumer.
Research limitations/implications – In this work, the authors address only one case stemming from the German automotive sector.
Practical implications – Technical enforcement of data providers policies instead of relying on trust to support collaborative data exchange between companies.
Originality/value – This research is among the first to introduce architecture options that provide a technical concept for the implementation of data sovereignty in business ecosystems using UC. Consequently, it supports the decision process for the technical implementation of data sovereignty.

Keywords Architecture, Business ecosystem, Design science research, Data sovereignty, Usage control

Paper type Research paper

1. Introduction

The on-going digitization process of the industrial sectors brings with it disruptive developments for how enterprises conduct business. The explosion of the volume of data influences business models at their core. In the digital world, enterprises need to build business ecosystems to be able to share data to provide products and services (Acatech *et al.*, 2014). A central issue with data is the simplicity with which they are copied or shared. For example, in the music industry, songs in MP3 format can easily be

This research was supported by the Excellence Center for Logistics and IT funded by the Fraunhofer-Gesellschaft and the Ministry of Culture and Science of the German State of North Rhine-Westphalia and by the International Data Spaces (IDS) initiative funded by the German Ministry for Education and Research.

Journal of Enterprise Information Management
Vol. 32 No. 3, 2019
pp. 477-495
© Emerald Publishing Limited
1741-0398
DOI 10.1108/JEIM-03-2018-0058

shared between people without taking into consideration the owner's copyrights (Ma, 2017). Business will grow ever more codependent and form digital business ecosystems. Therefore, the questions about the capabilities of being self-determined concerning its data will become more critical for businesses. The required capabilities are summarized under the term data sovereignty (Otto *et al.*, 2017). Business partners do not only need to specify access rights toward shared data but also need to set usage control (UC) policies, which specify how third parties can use their data (Karafili and Lupu, 2017).

Sharing data between enterprises is a complex issue entangled with multiple requirements, which need to be molded into policies. The design of well-formulated data usage policies is of paramount importance for beneficial cooperation in a business ecosystem. For example, it is not sufficient to specify who can access which data, but it is also necessary to specify for what amount of time a third party can access and utilize the data (Pearson and Casassa-Mont, 2011).

Despite the existing architecture for decentral search from Lablans *et al.* (2015) and the encryption-based solution for federated clouds from Esposito *et al.* (2016), there is no technical concept on how to implement data sovereignty. So far no research considers business ecosystems and UC in the context of data sovereignty. However, as business ecosystems become ever more relevant, the way of implementing data sovereignty by UC needs to be addressed.

The authors present a conceptual framework, i.e., architecture options, for the realization of UC policies between an original equipment manufacturer (OEM) and a Tier-1 supplier (from now on referred to as "supplier") in the German automotive industry to enforce data sovereignty. The focus on the automotive industry is deliberately chosen because it is the largest and highly developed branch of industry in Germany, which has to implement a closer collaboration of the participating companies in order to remain competitive (Henke and Kuhn, 2017).

The work is based on the "Collaborative Supply Chain Risk Management" (CSCRM) use case from the industrial data space (IDS). The IDS is an initiative to foster and implement data sovereignty in business ecosystems. The IDS delivers a reference architecture giving a conceptual representation for inter-organizational data exchange entangled with policies and rules (Otto *et al.*, 2018).

Through analysis of literature and assertion of problems in the field, the authors specify policies, which the architecture options need to represent and to enforce. In this analysis, the authors take into account the exchange of sensitive data between the two parties. For this, various levels of security and implementations give possible architecture options.

The authors address the following research questions (RQ):

RQ1. What are requirements for data sovereignty and UC policies in the use case CSCRM?

RQ2. What architecture options exist to enable UC and how can they be compared regarding practical implementation?

The authors investigate the RQs through rigorous literature review and a case study with practitioners, which ensures scientific rigor on one hand and relevancy for the field on the other.

The paper is structured as follows: Section 2 introduces the relevant terminologies and related concepts in the field of UC. In Section 3 the authors present their research design, which draws from design science research (DSR), case study research and workshops. Section 4 introduces requirements for data sovereignty and UC. Following, the authors present their architecture options for UC implementation in Section 5. Building on that, Section 6 demonstrates and evaluates the architecture options.

2. Background and related work

2.1 Approach for literature review

The following section presents the state of the art of business ecosystems, data sovereignty and concepts for data policy enforcement. The review follows established guidelines outlining the form of the literature review. Thus, the authors collected data from established scientific databases like Scopus, IEEE and Jstor. Both conference proceedings as well as journals are taken into consideration, as well as corresponding referenced documents (backward search) and citing documents (forward search) (Webster and Watson, 2002). The topics above define the search terms, which include the keywords "business ecosystem," "data sovereignty," "data policy enforcement," "usage control" and "data usage." The search is conducted in abstracts, titles and keywords (Vom Brocke *et al.*, 2015).

2.2 Business ecosystem

A business ecosystems consist of a multitude of actors, which share a common fate in an economic network (Moore, 2006). Actors in the business ecosystem are usually organizations, e.g., universities, large corporations or small firms. Cooperation, as well as competition, are both inherent characteristics of the business ecosystems (Peltoniemi and Vuori, 2004). Some authors explicitly mention digital ecosystems and characterize it as being a dynamic open community without centralized control or a rigid hierarchy (Boley and Chang, 2007; Chang and West, 2006). Therefore, the participants of an ecosystem are connected through a peer-to-peer network (Briscoe and Marinos, 2009). Nachira (2002) introduces digital business ecosystems with a strong emphasis on pervasive software to support business services and facilitate self-organizing behavior. For the remainder of the paper, the authors focus on the definition given by Moore and adopt the terminology business ecosystem.

2.3 Data sovereignty

Data sovereignty is a young field of scientific research and lacks a universal definition (Polatin-Reuben and Wright, 2014). Some researchers focus their research on data sovereignty in specific domains. These are national data sovereignty (Amoore, 2018; Hippelainen *et al.*, 2017; Nugraha *et al.*, 2015; Esposito *et al.*, 2016; Polatin-Reuben and Wright, 2014; Irion, 2012; Peterson *et al.*, 2011), medical data (Lablans *et al.*, 2015) and data sovereignty in cloud architecture options (Choo, 2014; Esposito *et al.*, 2016; Forrester, 2015).

In the context of national jurisdiction, data sovereignty refers to data being subject to the local law (Polatin-Reuben and Wright, 2014; Hippelainen *et al.*, 2017). Further, it refers to the government having full authority over virtual public data (Irion, 2012) and if it is the law of the land, must not leave its borders (Amoore, 2018). Peterson argues that data sovereignty refers to data being confined to the borders of the respective country (Peterson *et al.*, 2011). A related research field is data residency, which addresses "[…] the location of data and metadata, the movement of (meta)data across geographies and jurisdictions, and the protection of that (meta)data […]" (Object Management Group, 2017). In their discussion paper, the authors state potential pitfalls due to different economic policies, legislation and regulations of various countries and states besides implementation challenges.

Lablans *et al.* (2015) provide architecture for searching information in distributed databases. Their goal is to exchange data between medical facilities without violating one's data sovereignty. While they do not give an explicit definition, it is evident that they intend to regulate usage as well as access of data, i.e., to give the data owner a high level of control. Forrester conducted a survey investigating which approaches to manage data sovereignty are already in use by practitioners and which are still in planning (Forrester, 2015).

Otto *et al.* (2017) give a general definition of data sovereignty and state that data sovereignty can be defined as "a natural person's or corporate entity's capability of being entirely self-determined with regard to its data". The authors adopt the definition given by Otto *et al.* for the remainder of this paper.

Some architecture concepts for data sovereignty exist in the literature. For example the concept for decentral search from Lablans *et al.* (2015) and the encryption-based solution for federated clouds from Esposito *et al.* (2016). Yet, there is no technical concept on how to implement data sovereignty, especially not in a business ecosystem. It thus remains a need to specify architecture options for data sovereignty in a business ecosystem.

2.4 Concepts for data policy enforcement

Different concepts for data policy enforcement try to tackle security issues given by the intangible nature of digital content. The authors present digital rights management (DRM) as a concept for distributing digital content through enforcing digital licenses, data leakage prevention (DLP) as a concept to prevent leakage of sensitive information and access control (AC). Based on that the authors introduce UC and its relationship toward DRM and DLP (see Table I).

UC describes rules for usage of data between the provider of the data and the customer. Four parties can determine the rules: these are data owner, data provider, government and a previous owner (Pretschner *et al.*, 2006). Consumer-side mechanism enforces the previously negotiated terms of usage (Pretschner *et al.*, 2008). UC is a concept summarizing and extending the scope of different approaches to data policy enforcement, like AC, DRM and trust management (Park and Sandhu, 2002). Park *et al.*, contextualize UC with DRM, AC and trust management. While the previously mentioned approaches focus on specific aspects (privacy protection, intellectual property rights protection, sensitive information protection) UC takes a comprehensive approach. Their work further produced the UCON$_{ABC}$ Model conceptualizing UC into a model consisting of eight core components, namely, authorizations, objects, conditions, obligations, subjects, rights, object attributes and usage decision (Park and Sandhu, 2004).

Contrary to traditional AC, UC does not stop at merely regulating access but also controls future usage of data by adding restrictions (Jung *et al.*, 2014; Kelbert and Pretschner, 2012; Pretschner *et al.*, 2008). In other words, AC handles the rights to acquire data and UC specifies how the recipient may utilize the date (Bussard *et al.*, 2010). That relates to UC incorporating elements of DRM (Huang *et al.*, 2013). If UC is applied onto a distributed system, i.e., a network of actors (e.g. an information system or processing device) then it is defined as distributed UC (Pretschner *et al.*, 2006).

Some approaches for UC exist in the literature. Gheorghe *et al.* (2010) provide the enterprise service bus (ESB) model. Their approach intersects between different services in

	Description	Literature
DRM	Management of usage of digital content through digital licenses	Frattolillo (2017), Lin *et al.* (2005), Ma (2017), Liu *et al.* (2003), Stamp (2003), Elshazly *et al.* (2017)
DLP	Proactive approach to prevent leakage of sensitive data	Alneyadi *et al.* (2016), Katz *et al.* (2014), Wu *et al.* (2011), Stamati-Koromina *et al.* (2012)
AC	Specifies conditions under which a party can access data	Sandhu and Samarati (1994), Sandhu (1993), Goyal *et al.* (2006), Kalam *et al.* (2003)
UC	Combines DRM, DLP, and AC. Thus, UC provides rules for accessing and using data in addition to specifying ownership	Jung *et al.* (2014), Kumari and Pretschner (2012), Kelbert and Pretschner (2012), Bussard *et al.* (2010), Gheorghe *et al.* (2010), Pretschner *et al.* (2008), Pretschner *et al.* (2006), Sandhu and Park (2003), Park and Sandhu (2002)

Table I.
Concepts for data policy enforcement

a service-oriented architecture (SOA) option. The enforcement process of the ESB consists of three parts, namely interceptor (receives a message), decision maker (produces a verdict based on policy) and the action performer (producing the message based on the decision maker) (Gheorghe *et al.*, 2010).

Huang *et al.* (2013) present an approach for trusted UC of digital multimedia content based on cloud technology. Their framework includes a cloud security server, which manages security strategies and UC policies.

Based on the literature review, the authors identify the gap in research as follows. While some research takes into account aspects of business ecosystems, UC and data sovereignty, there is a lack of a comprehensive view of the three deeply interlaced contexts. As ecosystems and digital business solutions become ever more relevant, the question of how data sovereignty is realized in inter-organizational conduct needs to be answered. In this paper, the authors propose architectural options to implement data sovereignty through enforcing UC policies in business ecosystems.

3. Research design

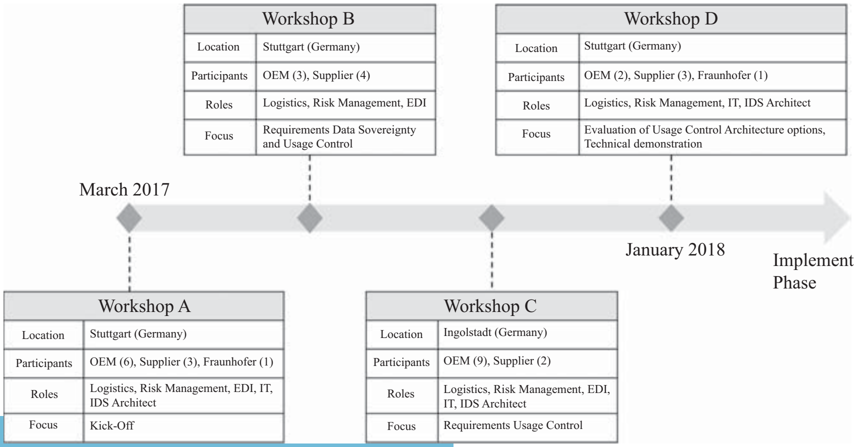
3.1 Case setting and description

The research in this paper develops conceptual architecture options for UC applications in the automotive, industrial context. It bases on the "CSCRM" use case stemming from the IDS consortium. The use case describes a project spanning from March 2017 up to January 2018 thematizing the automated exchange of sensitive data between an OEM and a supplier from the German automotive sector. Throughout the research effort, the authors conducted four workshops representing distinct milestones (see Figure 1).

The companies use IDS connectors, which are standardized interfaces for receiving, sending and transforming data sets for communication. They transmit the data from the connector to the target system (e.g. risk management system or supplier management system). Besides the actual data, data sets consist of metadata, which describes the nature of the data and the related usage policies (Otto *et al.*, 2017). Figure 2 shows the nature of the relationship between the OEM and the supplier as well as the IT-infrastructure enabling data exchange.

3.2 Case study design

Methodologically, the present paper reports on a single-case study. One can distinguish between case studies covering a single case, i.e., single-case studies and those covering



Workshop B	
Location	Stuttgart (Germany)
Participants	OEM (3), Supplier (4)
Roles	Logistics, Risk Management, EDI
Focus	Requirements Data Sovereignty and Usage Control

Workshop D	
Location	Stuttgart (Germany)
Participants	OEM (2), Supplier (3), Fraunhofer (1)
Roles	Logistics, Risk Management, IT, IDS Architect
Focus	Evaluation of Usage Control Architecture options, Technical demonstration

Workshop A	
Location	Stuttgart (Germany)
Participants	OEM (6), Supplier (3), Fraunhofer (1)
Roles	Logistics, Risk Management, EDI, IT, IDS Architect
Focus	Kick-Off

Workshop C	
Location	Ingolstadt (Germany)
Participants	OEM (9), Supplier (2)
Roles	Logistics, Risk Management, EDI, IT, IDS Architect
Focus	Requirements Usage Control

Figure 1. Timeline of workshops conducted in the span of the research effort

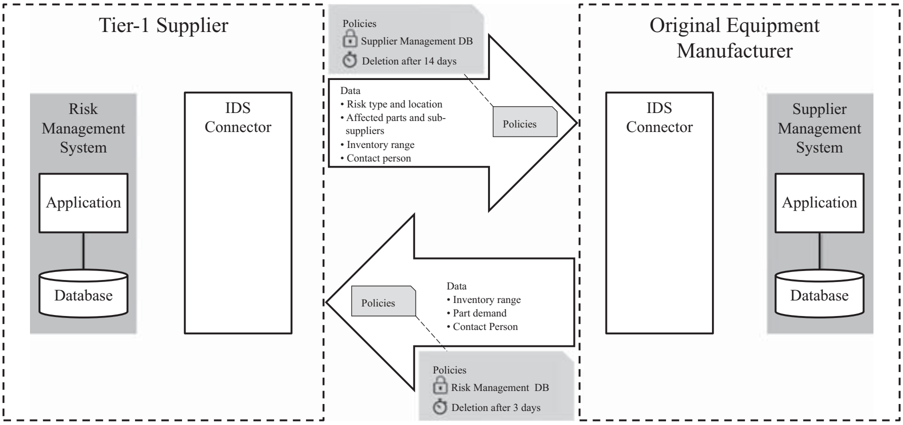


Figure 2.
IDS use case "CSCRM"

multiple cases, i.e. multiple-case studies (Gustafsson, 2017; Yin, 2008). Generally speaking, multiple-case studies provide a more fruitful basis for generalizing practical findings and abstracting scientific knowledge. However, the literature provides ample reasoning for focusing one's attention on a single case. Reasons for this being the opportunity to study a complex phenomenon in-depth and with greater focus as opposed to multiple cases (Gerring, 2004). As per the large-scale research effort situated in the German automotive industry and the thematization of a yet emerging and inherently complex field of research, the authors' reason that the nature of the given case is "extreme" and thus following a single-case strategy is not only suitable but purposeful (Gerring, 2006). In the following, the authors pursue reasoning based on logical argument, as well as an abstraction (Johansson, 2007). The case describes data exchange in the bilateral relationship between an OEM and a supplier, which, as a basic mode of inter-organizational networking, is common and a "representative case" across the automotive industry (Yin, 2008). In line with the recommendations of Yin and the encompassing warning of solely focusing on the representational character of the use case, it is the goal of the authors to produce abstracted design knowledge, i.e., theoretical knowledge in the form of data architecture options in business ecosystems (Yin, 2008). Thus, the present work entails high reusability through lifting practical instance problems into the realm of abstracted solutions and hence enhances applicability on further instance problems (Lee *et al.*, 2011). For the reasons above, the authors argue that following a single-case study research strategy is appropriate and goal oriented.

3.3 Design science research

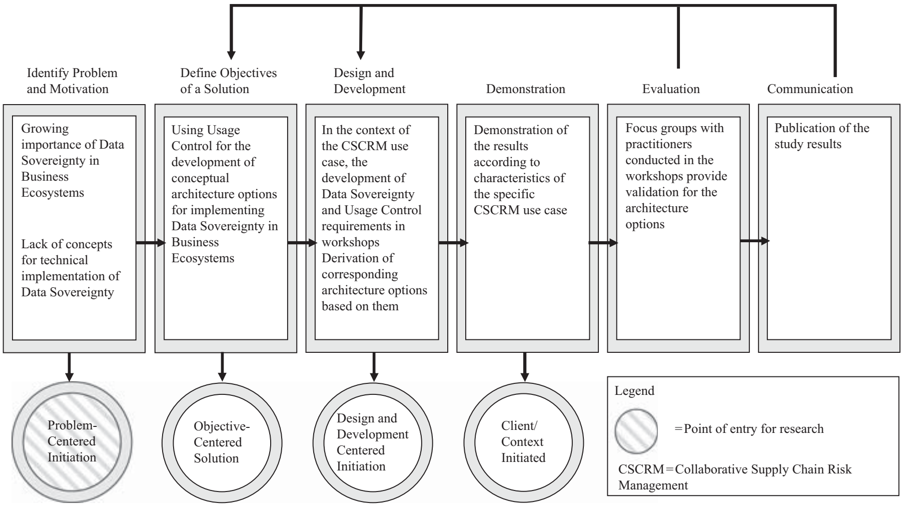
The authors use the DSR paradigm as proposed by Hevner *et al.* (2004) to develop the architecture options. DSR has gained increasing attention in the information systems research community and is a suitable paradigm for the development of novel IT-artifacts (Carlsson *et al.*, 2011). Peffers *et al.* provide the design science research methodology (DSRM) which offers a procedural model outlining the individual steps necessary toward generating an IT-artifact (Carlsson *et al.*, 2011). The procedural model consists of the following six steps, namely, identify problem and motivation, define objectives of a solution, design and development, demonstration, evaluation and communication (Peffers *et al.*, 2007). Typical artifacts, i.e., deliverables produced by DSR research projects are constructs, models, methods and instantiations (March and Smith, 1995). The proposed architecture options fall into the second category of DSR contribution types provided by Hevner and Gregor, as they classify as nascent design theory (Gregor and Hevner, 2013).

The authors follow the guidelines provided by Peffers *et al.* (2007) and thus begin with the first step identify problem and motivation. The motivation for the research conducted in this paper stems from input from the field as well as the literature. As presented in Section 2, there is a lack of a unified understanding of data sovereignty and a lack of data usage policies. The authors conducted three workshops to assert input regarding requirements of UC and data sovereignty. Figure 1 gives an overview of the conducted workshops. The design phase for the artifact predominantly bases on this mode data collection in workshops, focus groups and expert interviews conducted throughout the project duration. Focus groups provided the authors with the necessary tools to explore the mostly undiscovered scientific domain of data sovereignty and practice-oriented UC policies in the German automotive industry and to synthesize requirements (Rabiee, 2004; Tremblay *et al.*, 2010). Figure 3 gives an overview of each step taken. DSR offers various entry points for research projects. In the present case, the entry point is initiated through a problem, i.e., the lack of formal policies for inter-organizational data usage and their enforcement.

Second, the scope of this paper includes developing architecture options including the requirements and the resulting policies. The authors derive requirements for the architecture options by conducting interviews with experts from the automotive sector. Section 4 identifies the use case requirements for data sovereignty and UC policies.

Third, the authors develop the architecture options. Information systems architecture is a typical artifact in information systems research (Frank, 2000). The terminology initially sprung from the construction environment and describes complex structures being the sum of many individual parts (Ahlemann *et al.*, 2012). In IS research, architecture represents a model of an organizational information system, which describes rules, relationships and interfaces between individual components to cope with the ever-rising complexity of information systems (Leist and Zellner, 2006; Zachman, 1999). Possible architecture options on how to technically enforce the policies are developed in Section 5 and evaluated in Section 6.

Fourth, through the application of the architectural options onto an automotive, industrial use case, the authors show the feasibility and industrial applicability of the solutions. Using a single case yields the potential for intensive analysis of the object of observation (Gerring, 2004), which, e.g., can be a person or a system (Thomas, 2011).


Identify Problem and Motivation
Define Objectives of a Solution
Design and Development
Demonstration
Evaluation
Communication
Growing importance of Data Sovereignty in Business Ecosystems
Lack of concepts for technical implementation of Data Sovereignty
Using Usage Control for the development of conceptual architecture options for implementing Data Sovereignty in Business Ecosystems
In the context of the CSCRM use case, the development of Data Sovereignty and Usage Control requirements in workshops Derivation of corresponding architecture options based on them
Demonstration of the results according to characteristics of the specific CSCRM use case
Focus groups with practitioners conducted in the workshops provide validation for the architecture options
Publication of the study results
Problem-Centered Initiation
Objective-Centered Solution
Design and Development Centered Initiation
Client/ Context Initiated
Legend
▨ =Point of entry for research
CSCRM=Collaborative Supply Chain Risk Management

Source: Peffers *et al.* (2007)

Figure 3.
DSR Methodology as applied in the present research

While there is still much discussion in the literature about limitations of single-case studies regarding generalizability and compatibility (Flyvbjerg, 2006), it enables the development of complex solutions (see Section 3.2) (Eisenhardt and Graebner, 2007).

The authors follow March and Smith, who propose that evaluate results from design-oriented research through the development of suited criteria and the artifacts performance (March and Smith, 1995). Thus the authors analyze the suitability of the architecture in context to the *a priori* defined requirements (Frank, 2000). Additionally, the authors collect feedback focus groups of experts in the automotive sector. Figure 1 gives a timeline of all workshops conducted in the research effort. Each workshop represents a milestone in the project duration.

4. Requirements for data sovereignty and usage control policies

In this section, the authors analyze existing literature for data sovereignty and usage control policies requirements. Furthermore, they conduct a case study to survey requirements from the industry.

4.1 Requirements for data sovereignty

In the literature, the requirements for data sovereignty focus on checking and verifying the geolocation of the data because of possible legal issues in some countries (e.g. Esposito *et al.*, 2016; Amoore, 2018; Polatin-Reuben and Wright, 2014). Peterson *et al.* (2011) specify that requirement in "proofing the location of the server, where the data is stored" and "proofing if the data is stored at that server." Hippelainen *et al.* (2017) describe server location detection requirements from the data protection legislation, commercial constraints, cloud provider, cloud customer, extern auditor and cheating pattern perspective.

Table II shows the data sovereignty requirements for the IDS use case CSCRM which have been elicited during the workshops from practitioners.

4.2 Requirements for usage control policies

In general, UC policies define requirements on how data consumers are allowed to use the data (Pretschner *et al.*, 2006). There are two different types of UC requirements, namely provisions and obligations. Provisions impose AC requirements, for example, through specifying a necessary user role such as "manager" (Hilty *et al.*, 2005). Obligations represent

Requirements	Description
Simple definition and allocation of policies	The definition and enforcement of usage control policies have to be able with simple programming or customizing
Transparent processes	The usage control processes have to be transparent and comprehensible to the users
Short loading times	The loading time for the received data within the application has to be short (less than 3 seconds)
Parallel processing of many requests	Many users should be able to access the received data at the same time
Scalability	Data sovereignty needs to be scalable to realize the required usage control policies
Affordable for small- and medium-sized enterprises (SMEs)	SMEs have to be able to afford the necessary policy enforcement components for data sovereignty
Compatibility with all connectors from other companies	Data sovereignty has to work even if data provider and data consumer have connectors with different characteristics (e.g. manufacturer, release, size)
Manual intervention for data provider possible	The data provider can change the usage control policies manually because of special conditions (e.g. disaster)

Table II.
Requirements for data sovereignty from IDS use case "CSCRM"

future requirements that the data customer is bound to fulfill. Examples of obligations are "Data must not be stored more than 20 days" or "data must not be distributed" (Pretschner *et al.*, 2006). Obligations are classified according to two dimensions. If the obligation includes a fixed time interval or an infinitely valid condition, it is part of the dimension time. The second dimension is "observability" and covers the possibility to observe the violation of an obligation (Hilty *et al.*, 2005).

Requirements are enforced if the respective mechanisms are employed (Pretschner *et al.*, 2006). Mechanisms are installed on the data customer side and consist of a trigger event and an action (Pretschner *et al.*, 2008). A policy consists of one or more requirements. If at least one requirement is violated, then the policy agreement is breached (Pretschner *et al.*, 2006).

UC policies differentiate into specification-level policies (SLPs) and implementation-level policies (ILPs) (Rudolph *et al.*, 2016). SLPs describe policies through human-readable natural language and thus lack a common formalism. Contrary, the ILPs formalize SLPs and make them processable by a machine, i.e., machine-readable. Kumari and Pretschner (2012) describe the different enforcement possibilities for the requirement "picture must not be copied without notification." Similar examples can be drawn for a file delete-operation. For instance, the deletion of a file can mean: moving the file to the trash bin (e.g. Windows operating system), removing the reference of the file from the file system table, or overwriting the file location on the hard disk. SLP usually are imprecise, and thus the enforcement of policies is ambiguous. Hence, an SLP can be expressed through a combination of different ILPs achieving the same requirement. Rudolph *et al.* (2014) describe a method to support the elicitation of security policy requirements and transform them into security policy templates.

For identifying the UC policies for the IDS use case CSCRM the authors follow the security policy elicitation method from Rudolph *et al.* (2014). With all relevant stakeholders (see Section 3), SLP in natural language is developed and listed in Table III following the classification of Hilty *et al.* (2005). The authors decided to drop the second dimension of obligation ("observability") because non-observable events can be transferred to observable

		Obligations		
	Provisions	Fixed time interval	Eternally valid	Supporting literature
OEM as data provider	It is prohibited that the supplier imports the received data in another system than "Supply Chain Risk Database" It is prohibited that the supplier gives data access to employees with none of the roles "risk manager," "team leader logistics" or "sales representative for the affected parts"	It is obligatory that the supplier deletes the received data after three days	It is prohibited that the supplier forwards the received data to other companies It is prohibited that the supplier uses the received data for other purposes than risk and bottleneck management It is prohibited that the supplier uses the received data to the detriment of the OEM	Pearson and Casassa-Mont (2011), Gheorghe *et al.* (2010), Hilty *et al.* (2005)
Supplier as data provider	It is prohibited that the OEM imports the received data in another system than "Supplier Management Database" It is prohibited that the OEM gives data access to employees with none of the roles "risk manager," "dispatcher for the affected parts" or "purchaser for the affected parts"	It is obligatory that the OEM deletes the received data after 14 days	It is prohibited that the OEM forwards the received data to other companies It is prohibited that the OEM uses the received data for other purposes than risk and bottleneck management It is prohibited that the OEM uses the received data to the detriment of the supplier	

Table III.
Usage control policies from the IDS use case "CSCRM"

ones (Hilty *et al.*, 2005). The authors formulate policies according to the Semantics of Business Vocabulary and Business Rules (SBVR) from the Object Management Group (Object Management Group, 2016).

5. Usage control architecture options in business ecosystems

The following section comprises an introduction to the used policy enforcement framework and the different architecture options to implement data sovereignty by using this framework.

5.1 Policy enforcement framework

There are different approaches on how to cope with data UC and policy enforcement in general (see Section 2.4). Many policy enforcement solutions are based on the language and actors in the domain of XACML (eXtensible Access Control Markup Language), which represents an XML schema for authorization policies (OASIS, 2013). The main components and data flow in the XACML reference architecture are described below and depicted in Figure 4.

Policy administration point writes machine-readable policies and make them available to the PDP. With these policies, security administrators can specify their data sovereignty demands.

The policy enforcement point (PEP) receives data flow requests and demands a decision from the PDP how to proceed with the request. Depending on this decision, the PEP allows or denies the data flow.

The policy decision point (PDP) determines the decision for the data access request based on the installed policies. Policy evaluation may require additional information provided by a policy information point (PIP). Information returned by a PIP, which is not present in the request itself, may range from supplements from external services to data provided by a database.

The policy enforcement frameworks Integrated Distributed Data Usage Control Enforcement (IND^{2}UCE) uses the XACML approach shown in Figure 4, not only to cope with authorization but also with UC, which is essential for implementing data sovereignty. Therefore, IND^{2}UCE made changes to the architecture, the responsibility, and functionality of components (Steinebach *et al.*, 2016). For example, the PEPs in the IND^{2}UCE framework allows the modification of data in transit and therefore extend the PDP decision. Also, IND^{2}UCE allows that a decision can be bound to the successful execution of a specified action, such as the writing of a permanent log entry. In this case, the PDP triggers the execution of specified actions at a policy execution point (PXP). Only after successful execution has been acknowledged, the PDP will return the appropriate decision to the PEP; otherwise, a fallback action, if specified, will be performed.

The authors decided for IND^{2}UCE due to its mature state, its applicability to cope with the identified data sovereignty challenges and because it is one of the UC technologies used

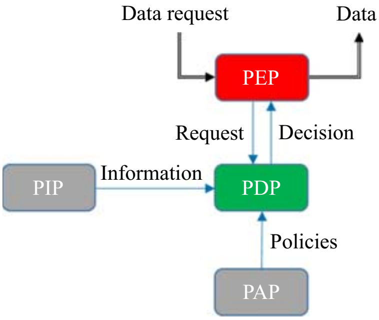


Figure 4. Simplified XACML architecture

Source: OASIS (2013)

in the IDS. The policy framework provides theoretical concepts and technological components for implementing data UC. Besides, it is actively researched in former and current research projects, and its applicability has been shown in different prototypical implementations. For more information about IND^{2}UCE refer to (Steinebach *et al.*, 2016).

The following will focus on a minimal set of IND^{2}UCE components to enforce the usage policies: the PDP for decision making, the PEP for intercepting data flows and the PXP for executing actions at the target system or platform.

5.2 Architecture options

The IDS use case "CSCRM" consists of two-sided data exchange between OEM and supplier. The authors describe the developed architecture options based on the one-way data exchange where the data store and policy enforcement components are located at the supplier (data consumer) side. The other option, when the OEM is data consumer, would be described analogically.

While considering the implementation of policy enforcement in a business ecosystem such as the IDS, the authors identified two basic dimensions that need to be investigated to develop an architecture based on the requirements from Section 4.

Data and its location are important factors for architectural design decisions (Naab *et al.*, 2015). Therefore, the first dimension is about the location, where the data consumer stores the received data from the provider. Furthermore, architectural design is always a tradeoff decision between cost and benefit (Kazman *et al.*, 2001). Thus, the second dimension is about what policy enforcement components are necessary and where they are located within the IT infrastructure.

Regarding the first dimension, the location of the data store can be in the application database, in an application independent database and in a database inside the IDS connector. From a theoretical point of view, it is possible to split the data storage up into different parts and implement all three characteristics at the same time. Regarding the technical implementation, the data provider would choose the appropriate approach from which the desired degree of data sovereignty can be achieved with acceptable effort.

Regarding the second dimension, the location of policy enforcement components can be in the connector, in the connector and database, in the connector, database, and application and in the connector, database, application and operating system. It is also possible to implement the policy enforcement components just in the application or just in the database, but from a data sovereignty perspective, stages are more appropriate to illustrate the capabilities and limits of UC.

Both dimensions have various characteristics, and their combination is critical regarding the capability of policy enforcement. Each combination goes along with advantages and disadvantages for the data consumer and provider.

When combining the dimensions, different levels of data sovereignty are possible.

Architecture option 1a and 2a (see Figure 5) store their data in the application or an independent database (1) whereas the enforcement components are in the connector (a). The PEP controls the data flow within the IDS connector. The PXP performs actions at the database and therefore gets access rights to trigger delete operations at the application database (1a) or the independent database (2a). These architectures enable only a low degree of data sovereignty for the data provider because the success of the delete operation or the further distribution of the data cannot be controlled.

Architecture option 3a and 3b store their data in a database inside the IDS connector and demand the implementation of enforcement components within the connector and the database. As the PEP controls the data flow within the IDS connector, it can modify or restrict access to data that is requested. The PXP is also able to perform actions on the database. Although the data is separated, the data sovereignty is quite limited, because the

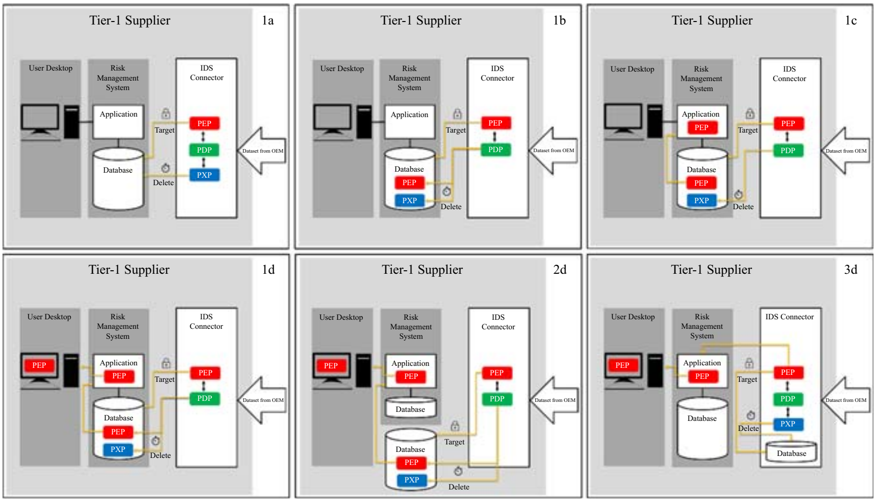


Figure 5.
Usage Control architecture options for data sovereignty

data which leave the connector, cannot be controlled as the application can process and archive the data without further control and tracking. Besides, the computation power and size of the database is also limited. Although 1b or 2b would probably solve the database issue, it moves the database out of a trusted environment.

In summary, the authors conclude that the highest level of data sovereignty is possible when the application is completely integrated into an ecosystem, where the transfer of all data is trace- and controllable. Implementing this approach results in high effort, high costs and causes some performance issues. Moving the application out of such an ecosystem lowers effort, costs and performance reduction with every step, but this holds for data sovereignty also. In the end, it is a tradeoff after considering all requirements.

The advantages and disadvantages of several combinations form a data consumer, and provider point of view are described in Table IV. The architecture options are illustrated in Figure 5. Because of space limitation, the authors focus on describing all architecture options with a data storage in the application database (1a, 1b, 1c and 1d) and exemplify the other two storage options only in the highest stage of UC enforcement (2d and 3d).

6. Evaluation

For evaluating the feasibility and industrial applicability of the developed architecture options, the authors perform a case study with practitioners from the automotive industry. Although representing different companies, the participants have taken on both perspectives, because they are both data providers and data consumers. In a one-day workshop (see Workshop D in Figure 1), the following steps are conducted as a focus group discussion: (Step 1) assessment of the most suitable architecture option for the CSCRM use case, (Step 2) discussion of implementation prerequisites and implications in practice, (Step 3) feasibility assessment of the architecture options. The discussion of all three steps is based on the data sovereignty requirements (see Table II) and the UC policies (see Table III) from Section 4.

Step 1: from a data provider perspective, the architecture option with the highest degree of data sovereignty is desirable. For a data consumer, an ideal solution is an architecture option with slightest implementation effort and performance issues, which still satisfies the requirements from the data provider. The data storage option inside the connector is the

Name	Data consumer	Data provider
1a	+ no system changes required + very low implementation costs – no separation between internal and external data	– no control of data access, distribution and deletion – no data manipulation is traceable – no control of data presentation – no prevention of screenshots and prints – no prevention of data archiving and shoulder surfing
1b	+ no application changes required + low implementation costs – no separation between internal and external data – database changes required – very small performance reduction (additional security queries)	+ control of data access, distribution and deletion + data manipulation is traceable – control of data presentation – prevention of screenshots and prints – no prevention of data archiving and shoulder surfing
1c	– no separation between internal and external data – database and application changes required – small performance reduction (additional security queries)	+ control of data access, distribution and deletion + data manipulation is traceable + control of data presentation – prevention of screenshots and prints – no prevention of data archiving and shoulder surfing
1d	– no separation between internal and external data – database, application and operating system changes required – medium performance reduction (additional security queries)	+ control of data access, distribution and deletion + data manipulation is traceable + control of data presentation + prevention of screenshots and prints – no prevention of data archiving and shoulder surfing
2d	+ separation between internal and external data – database, application and operating system changes required – medium performance reduction (additional security queries)	+ control of data access, distribution and deletion + data manipulation is traceable + control of data presentation + prevention of screenshots and prints – no prevention of data archiving and shoulder surfing
3d	+ separation between internal and external data + data is stored in a safe operating environment – database, application and operating system changes required – medium performance reduction (additional security queries)	+ control of data access, distribution and deletion + data manipulation is traceable + control of data presentation + prevention of screenshots and prints + prevention of data archiving – no prevention of shoulder surfing

Table IV. Comparison of selected usage control architecture options for data sovereignty

favored because there are no deletion commands from the connector to an internal database necessary. In sum, the practitioners found consensus in choosing architecture option 3d. This option does not require any changes to the application database and offers the highest degree of data sovereignty. At the moment this option is too costly to realize because of the PEP integration into the existing application and operating systems. Option 3a requires minor changes in the application (additional connection to the connector) and still enables data sovereignty to a limited extent. The practitioners stated that 3a would be a good intermediate step for solving their data sovereignty demands in the CSCRM use case. However, the target state of 3d requires additional implementation prerequisites (see evaluation Step 2).

Step 2: prerequisite for the implementation of the architecture option 3d is a fast and low-cost integration of PEPs in the application and the operating systems. A retrofitting of a PEP in an existing infrastructure requires a lot of programming effort. Also, the integration possibilities may be limited (e.g. the application source code is not available). Therefore, PEPs should be an enclosed component of the software (for example in the enterprise resource planning system) from the beginning. As a result, the integration of a PEP is part of the customization of the ERP provider. Furthermore, the PEPs must be certified by a neutral organization to ensure data sovereignty effectiveness and the operability of the data provider and consumer.

Step 3: the architecture options and the comparison of their characteristics (see Table IV) supports the technical implementation of data sovereignty in a business ecosystem. They assist the negotiation process between a data provider and customer through standardizing and simplifying the complex issue of formulating usage policies for data.

7. Conclusion

The digitization of business brings with it new challenges for inter-organizational collaboration, e.g., in the exchange of data to develop digital products and services.

Resulting from that is a rising need for conceptualizing and implementing policies to regulate and organize data usage between enterprises. However, there is a lack of literature about data sovereignty in business ecosystems. Therefore, the goal of this research is to provide a technical concept for the implementation of data sovereignty in business ecosystems using UC.

Following the DSR process, the research is based on the "CSCRM" use case between an OEM and one supplier stemming from the German automotive sector. In total, the authors conduct four workshops with practitioners from both companies. Three of the workshops have the focus to assert input regarding requirements of UC and data sovereignty. The fourth workshop is a focus group of experts to collect feedback to the architecture options.

RQ1 addresses the requirements of data sovereignty and UC policies in the use case. The authors identified eight requirements for data sovereignty with the practitioners. For example, performance requirements such as the ability of parallel processing, fast data transmission and a reasonable and straightforward implementation are essential. Furthermore, process transparency and the option to manually adjust the UC policies are crucial. In literature, data sovereignty requirements focus only on checking and verifying the data's geolocation (see Section 4.1). Regarding *RQ1*, the author's research amounts to the formulation of six distinct requirements for data sovereignty (see Table II) and UC policies (see Table III) in the use case.

RQ2 deals with the design of architecture options to enable UC. Based on two distinctive dimensions, the authors developed twelve architecture options. The first dimension deals with the data storage location, and the second dimension covers the location of policy enforcement components. Each architecture option has different characteristics and meets different data sovereignty requirements. The architecture option with the highest degree of data sovereignty for the data provider requires the highest implementation effort for the data consumer. Based on a case study with IT experts from the automotive industry, the architecture options are evaluated. A consideration of the benefits and the associated effort is inevitable.

The research at hands provides multiple contributions both managerial and scientific. Regarding scientific contributions, the research extends and grows the knowledge base of the hitherto mostly unexplored domains of data sovereignty and UC. More specifically, the core of this paper addresses the notion of the Business Ecosystems in said domains and contributes to filling the existing gap of research in that area. Moreover, through abstracting technical architecture options for UC, the authors argue that the research gives academics guidance in applying the concepts onto their respective domains.

Additionally, the present research makes a threefold managerial contribution. First, it increases the understanding of data sovereignty by describing requirements form the industrial context. Furthermore, the paper may help to shape the imagination and expectation regarding the opportunities with the use of UC and the corresponding policies for business to business collaboration. Finally, the architecture options support the implementation process of data sovereignty by demonstrating the characteristics of different approaches.

The limitation of this paper is the narrowing on one use case from the automotive industry. The input comes from two companies and their IT and logistics experts. The authors do not claim for cross-sector validity, but the results of this paper are the first step. However, it is a valid field for future research to evaluate the architecture options in other industries.

References

Acatech, Kagermann, H., Riemensperger, F., Hoke, D., Helbig, J., Stocksmeier, D., Wahlster, W., Scheer, A.-W. and Schweer, D. (2014), "Smart service welt. Umsetzungsempfehlungen für das Zukunftsprojekt Internetbasierte Dienste für die Wirtschaft", acatech – Deutsche Akademie der Technikwissenschaften, Berlin.

Ahlemann, F., Stettiner, E. and Messerschmidt, M. (2012), *Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments, Management for Professionals*, Springer, Berlin and Heidelberg.

Alneyadi, S., Sithirasenan, E. and Muthukkumarasamy, V. (2016), "A survey on data leakage prevention systems", *Journal of Network and Computer Applications*, Vol. 62 No. C, pp. 137-152.

Amoore, L. (2018), "Cloud geographies: computing, data, sovereignty", *Progress in Human Geography*, Vol. 42 No. 1, pp. 4-24.

Boley, H. and Chang, E. (2007), "Digital ecosystems: principles and semantics", *Inaugural IEEE-IES Digital EcoSystems and Technologies Conference, IEEE, Cairns, February 21-23*, pp. 398-403.

Briscoe, G. and Marinos, A. (2009), "Digital ecosystems in the clouds: towards community cloud computing", *3rd IEEE International Conference on Digital Ecosystems and Technologies, Piscataway, IEEE, Istanbul, July 1-3*, pp. 103-108.

Bussard, L., Neven, G. and Preiss, F.-S. (2010), "Downstream usage control", *IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), IEEE, Piscataway, NJ, July 21-23*, pp. 22-29.

Carlsson, S.A., Henningsson, S., Hrastinski, S. and Keller, C. (2011), "Socio-technical IS design science research: developing design theory for IS integration management", *Information Systems and e-Business Management*, Vol. 9 No. 1, pp. 109-131.

Chang, E. and West, M. (2006), "Digital ecosystems a next generation of the collaborative environment", *International Conference on Information Integration and Web-based Applications Services, Yogyakarta, December 4-6*.

Choo, K.-K.R. (2014), "Legal issues in the cloud", *IEEE Cloud Computing*, Vol. 1 No. 1, pp. 94-96.

Eisenhardt, K.M. and Graebner, M.E. (2007), "Theory building from cases. Opportunities and challenges", *Academy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

Elshazly, A.R., Nasr, M.E., Fouad, M.M. and Abdel-Samie, F.S. (2017), "High payload multi-channel dual audio watermarking algorithm based on discrete wavelet transform and singular value decomposition", *International Journal of Speech Technology*, Vol. 20 No. 4, pp. 951-958.

Esposito, C., Castiglione, A. and Choo, K.-K.R. (2016), "Encryption-based solution for data sovereignty in federated clouds", *IEEE Cloud Computing*, Vol. 3 No. 1, pp. 12-17.

Flyvbjerg, B. (2006), "Five misunderstandings about case-study research", *Qualitative Inquiry*, Vol. 12 No. 2, pp. 219-245.

Forrester (2015), "Data sovereignty and SaaS: understanding the challenges and regulatory requirements", available at: www.intralinks.com/resources/whitepapers/data-sovereignty-and-saas (accessed May 1, 2019).

Frank, U. (2000), "Evaluation von Artefakten in der Wirtschaftsinformatik", in Häntschel, I. and Heinrich, L.J. (Eds), *Evaluation und Evaluationsforschung in der Wirtschaftsinformatik*, München, pp. 35-48.

Frattolillo, F. (2017), "A digital rights management system based on cloud", *Telkomnika (Telecommunication Computing Electronics and Control)*, Vol. 15 No. 2, pp. 671-677.

Gerring, J. (2004), "What is a case study and what is it good for?", *American Political Science Review*, Vol. 98 No. 2, pp. 341-354.

Gerring, J. (2006), *Case Study Research: Principles and Practices*, Cambridge University Press, Cambridge.

Gheorghe, G., Mori, P., Crispo, B. and Martinelli, F. (2010), "Enforcing UCON policies on the enterprise service bus", in Meersman, R., Dillon, T. and Herrero, P. (Eds), *On the Move to Meaningful Internet Systems: OTM 2010: Confederated International Conferences: CoopIS, IS, DOA and ODBASE, Hersonissos, Crete*, *Springer*, *Berlin*, *Proceedings, Part II, October 25-29*, pp. 876-894.

Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006), "Attribute-based encryption for fine-grained access control of encrypted data", in Juels, A., Wright, R. and Di Capitani Vimercati, S. de (Eds), *Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, Virginia, ACM, New York, NY*, p. 89.

Gregor, S. and Hevner, A.R. (2013), "Positioning and presenting design science research for maximum impact", *MIS Quarterly*, Vol. 37 No. 2, pp. 337-355.

Gustafsson, J. (2017), "Single case studies vs. multiple case studies: a comparative study", available at: www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf (accessed May 1, 2019).

Henke, M. and Kuhn, A. (Eds) (2017), *Kollaboration als Schlüssel zum erfolgreichen Transfer von Innovation: Analyse von Treibern und Hemmnissen in der Automobillogistik*, Herbert UTZ, München.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MIS Quarterly: Management Information Systems*, Vol. 28 No. 1, pp. 75-105.

Hilty, M., Basin, D. and Pretschner, A. (2005), "On Obligations", in Di Capitani Vimercati, S., de, Gollmann, D. and Syverson, P. (Eds), *Computer Security – ESORICS 2005: 10th European Symposium on Research in Computer Security, Milan, Proceedings, Lecture Notes in Computer Science*, Springer, *Berlin and Heidelberg*, *September 12-14*, pp. 98-117.

Hippelainen, L., Oliver, I. and Lal, S. (2017), "Towards dependably detecting geolocation of cloud servers", in Tally, R.T., Battista, C.M., Yan, Z., Molva, R., Mazurczyk, W. and Kantola, R. (Eds), *Ecocriticism and Geocriticism/Network and System Security: Overlapping Territories in Environmental and Spatial Literary Studies/11th International Conference, NSS 2017, Helsinki*, *Proceedings, Geocriticism and Spatial Literary Studies, Palgrave Macmillan*; *Springer*, *New York*, *August 21-23*, pp. 643-656.

Huang, T., Zhang, Z., Chen, Q. and Chang, Y. (2013), "A method for trusted usage control over digital contents based on cloud computing", *International Journal of Digital Content Technology and its Applications*, Vol. 7 No. 4, pp. 795-802.

Irion, K. (2012), "Government cloud computing and national data sovereignty", *Policy & Internet*, Vol. 4 Nos 3-4, pp. 40-71.

Johansson, R. (2007), "On case study methodology", *Open House International*, Vol. 32 No. 3, pp. 48-54.

Jung, C., Eitel, A. and Schwarz, R. (2014), "Enhancing cloud security with context-aware usage control policies", in Plödereder, E., Grunske, L., Schneider, E. and Ull, D. (Eds), *44. Jahrestagung der Gesellschaft für Informatik: Big Data – Komplexität meistern*, GI, Stuttgart, pp. 211-222.

Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C. and Trouessin, G. (2003), "Organization based access control", *Proceedings, POLICY 2003: IEEE 4th International Workshop on Policies for Distributed Systems and Networks, IEEE, Lake Como*, *June 4-6*, pp. 120-131.

Karafili, E. and Lupu, E.C. (2017), "Enabling data sharing in contextual environments. Policy representation and analysis", *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, ACM*, *New York, NY*, pp. 231-238.

Katz, G., Elovici, Y. and Shapira, B. (2014), "CoBAn: a context based model for data leakage prevention", *Information Sciences*, Vol. 262, pp. 137-158.

Kazman, R., Asundi, J. and Klein, M. (2001), "Quantifying the costs and benefits of architectural decisions", *Proceedings of the 23rd International Conference on Software Engineering: ICSE, IEEE Computer Society, IEEE*, *Toronto*, *May 12-19*, pp. 297-306.

Kelbert, F. and Pretschner, A. (2012), "Towards a policy enforcement infrastructure for distributed usage control", in Atluri, V. (Ed.), *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, ACM, New York, NY*, pp. 119-122.

Kumari, P. and Pretschner, A. (2012), "Deriving implementation-level policies for usage control enforcement", in Bertino, E. (Ed.), *Proceedings of the Second ACM Conference on Data and Application Security and Privacy*, *ACM*, *New York, NY*, *February 7-9*, p. 83.

Lablans, M., Kadioglu, D., Muscholl, M. and Ückert, F. (2015), "Exploiting distributed, heterogeneous and sensitive data stocks while maintaining the owner's data sovereignty", *Methods of Information in Medicine*, Vol. 54 No. 4, pp. 346-352.

Lee, J.S., Pries-Heje, J. and Baskerville, R. (2011), "Theorizing in design science research", in Jain, H., Sinha, A.P. and Vitharana, P. (Eds), *Service-Oriented Perspectives in Design Science Research*, Springer, Berlin and Heidelberg, pp. 1-16.

Leist, S. and Zellner, G. (2006), "Evaluation of current architecture frameworks", *Proceedings of the ACM Symposium on Applied Computing*, *Dijon*, *April 23-27*, pp. 1546-1553.

Lin, E.T., Eskicioglu, A.M., Lagendijk, R.L. and Delp, E.J. (2005), "Advances in digital video content protection", *Proceedings of the IEEE*, Vol. 93 No. 1, pp. 171-182.

Liu, Q., Safavi-Naini, R. and Sheppard, N.P. (2003), "Digital rights management for content distribution", *Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003 – Volume 21, Australian Computer Society, Darlinghurst*, pp. 49-58.

Ma, Z. (2017), "Digital rights management. Model, technology and application", *China Communications*, Vol. 14 No. 6, pp. 156-167.

March, S.T. and Smith, G.F. (1995), "Design and natural science research on information technology", *Decision Support Systems*, Vol. 15 No. 4, pp. 251-266.

Moore, J.F. (2006), "Business ecosystems and the view from the firm", *The Antitrust Bulletin*, Vol. 51 No. 1, pp. 31-75.

Naab, M., Braun, S., Lenhart, T., Hess, S., Eitel, A., Magin, D., Carbon, R. and Kiefer, F. (2015), "Why data needs more attention in architecture design – experiences from prototyping a large-scale mobile app ecosystem", in Bass, L., Lago, P. and Kruchten, P. (Eds), *12th Working IEEE/IFIP Conference on Software Architecture, WICSA 2015: Montréal*, *IEEE*, *Piscataway, NJ*, *May 4-8*, pp. 75-84.

Nachira, F. (2002), "Toward a network of digital business ecosystems fostering the local development", available at: www.digital-ecosystems.org/doc/discussionpaper.pdf (accessed May 1, 2019).

Nugraha, Y., Kautsarina, A.S. and Sastrosubroto, A.S. (2015), "Towards data sovereignty in cyberspace", *3rd International Conference of Information and Communication Technology*, *Piscataway, NJ*, *Nusa Dua and Bali*, *May 27-29*, pp. 465-471.

OASIS (2013), "eXtensible access control markup language (XACML) version 3.0", available at: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html (accessed January 16, 2018).

Object Management Group (2016), "Semantics of business vocabulary and business rules (SBVR)", available at: www.omg.org/spec/SBVR/About-SBVR/ (accessed May 1, 2019).

Object Management Group (2017), "Data residency challenges and opportunities for standardization", available at: www.omg.org/cgi-bin/doc?mars/17-03-22.pdf (accessed January 16, 2018).

Otto, B., Hompel, M.T. and Wrobel, S. (2018), "Industrial data space", in Neugebauer, R. (Ed.), *Digitalisierung: Referenzarchitektur für die Digitalisierung der Wirtschaft*, Springer, Berlin and Heidelberg, pp. 113-133.

Otto, B., Lohmann, S., Auer, S., Brost, G., Cirullies, J., Eitel, A., Ernst, T., Haas, C., Huber, M., Jung, C., Jürjens, J., Lange, C., Mader, C., Menz, N., Nagel, R., Pettenpohl, H., Pullmann, J., Quix, C., Schon, J., Schulz, D., Schütte, J., Spiekermann, M. and Wenzel, S. (2017), "Reference architecture model for the industrial data space", *International Data Space Association*, Fraunhofer-Geschsllschaft, available at: www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/IDS_Referenz_Architecture.pdf (accessed May 1, 2019).

Park, J. and Sandhu, R. (2002), "Towards usage control models. Beyond traditional access control", in Sandhu, R. (Ed.), *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies*, *ACM*, *New York, NY*, *June 3-4*, p. 57.

Park, J. and Sandhu, R. (2004), "The UCON ABC usage control model", *ACM Transactions on Information and System Security*, Vol. 7 No. 1, pp. 128-174.

Pearson, S. and Casassa-Mont, M. (2011), "Sticky policies: An approach for managing privacy across multiple parties", *Computer*, Vol. 44 No. 9, pp. 60-68.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007), "A design science research methodology for information systems research", *Journal of Management Information Systems*, Vol. 24 No. 3, pp. 45-77.

Peltoniemi, M. and Vuori, E. (2004), "Business ecosystem as the new approach to complex adaptive business environments", in Seppä, M., Hannula, M., Järvelin, A.-M., Kujala, J., Ruohonen, M. and Tiainen, T. (Eds), *Frontiers of e-Business Research-Conference Proceedings*, Tampere, pp. 267-281.

Peterson, Z.N.J., Gondree, M. and Beverly, R. (2011), "A position paper on data sovereignty. The importance of geolocating data in the cloud", *Proceedings of the 3rd Usenix Conference on Hot Topics in Cloud Computing*, *Portland, OR*, *June 14-15*, pp. 9-13.

Polatin-Reuben, D. and Wright, J. (2014), "An Internet with BRICS characteristics. Data sovereignty and the balkanisation of the Internet", 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14), USENIX Association, San Diego, CA.

Pretschner, A., Hilty, M. and Basin, D. (2006), "Distributed usage control", *Communications of the ACM*, Vol. 49 No. 9, pp. 39-44.

Pretschner, A., Hilty, M., Basin, D., Schaefer, C. and Walter, T. (2008), "Mechanisms for usage control", in Abe, M. (Ed.), *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, *ACM*, *New York, NY*, pp. 240-244.

Rabiee, F. (2004), "Focus-group interview and data analysis", *Proceedings of the Nutrition Society*, Vol. 63 No. 4, pp. 655-660.

Rudolph, M., Moucha, C. and Feth, D. (2016), "A framework for generating user-and domain-tailored security policy editors", *IEEE 24th International Requirements Engineering Conference workshops: Proceedings*, *IEEE*, *Piscataway, NJ*, *September 12-16*, pp. 56-61.

Rudolph, M., Schwarz, R. and Jung, C. (2014), "Security policy specification templates for critical infrastructure services in the cloud", *9th International Conference for Internet Technology and Secured Transactions*, *IEEE*, *Piscataway, NJ*, *December 8-10*, pp. 61-66.

Sandhu, R. and Park, J. (2003), "Usage control. A vision for next generation access control", in Gorodetsky, V., Popyack, L. and Skormin, V. (Eds), *Computer Network Security: Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2003, St Petersburg. Proceedings, Lecture Notes in Computer Science, Vol. 2776*, *Springer*, *Berlin and Heidelberg*, *September 21-23*, pp. 17-31.

Sandhu, R.S. (1993), "Lattice-based access control models", *Computer*, Vol. 26 No. 11, pp. 9-19.

Sandhu, R.S. and Samarati, P. (1994), "Access control. Principle and practice", *IEEE Communications Magazine*, Vol. 32 No. 9, pp. 40-48.

Stamati-Koromina, V., Ilioudis, C., Overill, R., Georgiadis, C.K. and Stamatis, D. (2012), "Insider threats in corporate environments. A case study for data leakage prevention", *ACM International Conference Proceeding Series*, *Novi Sad, Serbia*, *September 16-20*, pp. 271-274.

Stamp, M. (2003), "Digital rights management. The technology behind the hype", *Journal of Electronic Commerce Research*, Vol. 4 No. 3, pp. 102-112.

Steinebach, M., Krempel, E., Jung, C. and Hoffmann, M. (2016), "Datenschutz und datenanalyse", *Datenschutz und Datensicherheit – DuD*, Vol. 40 No. 7, pp. 440-445.

Thomas, G. (2011), "A typology for the case study in social science following a review of definition, discourse, and structure", *Qualitative Inquiry*, Vol. 17 No. 6, pp. 511-521.

Tremblay, M.C., Hevner, A.R. and Berndt, D.J. (2010), "The use of focus groups in design science research", in Hevner, A. and Chatterjee, S. (Eds), *Design Research in Information Systems: Theory and Practice*, Springer, Boston, MA, pp. 121-143.

Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R. and Cleven, A. (2015), "Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research", *CAIS*, Vol. 37, p. 9.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MIS Quarterly: Management Information Systems*, Vol. 26 No. 2, pp. xiii-xxiii.

Wu, J., Zhou, J., Ma, J., Mei, S. and Ren, J. (2011), "An active data leakage prevention model for insider threat", *Proceedings – 2011 International Symposium on Intelligence Information Processing and Trusted Computing, IEEE, Wuhan, October 22-23*, pp. 39-42.

Yin, R.K. (2008), *Case Study Research: Design and Methods*, 4th ed., Sage Publications, Thousand Oaks, CA.

Zachman, J.A. (1999), "Framework for information systems architecture", *IBM Systems Journal*, Vol. 38 No. 2, pp. 454-470.

Corresponding author
Johannes Zrenner can be contacted at: johannes.zrenner@tu-dortmund.de