H. Roßnagel et al. (Eds.): Open Identity Summit 2019,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019 119

The ENTOURAGE Privacy and Security Reference Architecture for Internet of Things Ecosystems

Jan Zibuschka[1] Moritz Horsch[2] Michael Kubach[3]

Abstract: The Internet of Things (IoT), with its ubiquitous sensors and actuators, enables highly useful novel use cases, notably in the field of digital assistance. It also raises unprecedented privacy and security issues. This contribution presents a reference architecture for an ecosystem of digital assistants with minimal barriers of entry, that aims to be both secure and privacy-respecting. We present concise definitions, requirements, and a layered architectural structure for IoT assistants. Moreover, we introduce privacy and security assistants building on privacy patterns such as privacy dashboard, privacy mode and security and privacy policies and interface.

Keywords: ecosystem; privacy; digital assistant; architecture; Internet of Things

1 Introduction

The Internet of Things (IoT) is upon us: countless sensing devices, equipped with sensors ranging from microphones to detectors for complex chemical compounds, are permeating our everyday lives. Perhaps the most prominent example for this is the smart phone, but devices such as smart watches and fitness trackers are similarly becoming commonplace. At the same time, devices equipped with actuators, such as the effectors in industrial robots, are becoming increasingly networked. There are also IoT product categories combining both sensors and actuators, such as connected cars or smart home appliances.

Controlling these myriad sensors and actuators is – simply for the fact that they are so numerous and the data streams transmitted between them are of such high volume – very challenging for the individual [To16]. Therefore, what is needed are digital assistants taking over part of the processing in place of the human, translating high level commands into individual effector movements and transforming various sensor outputs into a format that is digestible by the user. To reach a useful degree of automation, the assistants often have knowledge about the individuals preferences, schedules, and even biometrics. Such intelligent systems will clearly tend to employ machine learning and big data technologies.

[1] Robert Bosch GmbH, Zentralbereich Forschung und Vorausentwicklung, Renningen, 70465 Stuttgart, Deutschland; jan.zibuschka@de.bosch.com
[2] Technische Universität Darmstadt, Theoretische Informatik – Kryptographie und Computeralgebra, Hochschulstraße 10, 64289 Darmstadt, Deutschland; horsch@cdc.informatik.tu-darmstadt.de
[3] Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Team Identity Management, Allmandring 35, 70569 Stuttgart, Deutschland; michael.kubach@iao.fraunhofer.de

Once again, such digital assistants are readily found on devices from modern smart phones to connected cars [LQG17], and also in scenarios with many networked devices [Be15].

While the proliferation of IoT-enabled devices suggests a high usefulness for both individuals and organizations, this development is not without its challenges: in contrast to the standardized, open Internet, IoT systems are commonly not interoperable beyond the walled garden platforms of their manufacturers, and at best extensible in a plug-in manner. This is especially true for the assistants running on the IoT platforms. This raises both technological questions with regards to the mechanisms needed for interoperability, and organizational issues with regards to the construction of an open market for such assistants [KGH16]. Ethical aspects and regulation of such an open ecosystem are also not trivial. Specifically, while European privacy regulation has proven a solid defense for the individuals basic rights, and compliant privacy solutions for e.g. location based services are well-known [Ra07], the combination of IoT and assistants holds both new challenges and new possibilities for individual privacy, which need to be carefully investigated [KGH16].

Ecosystems have emerged as a area of research in various parts of the IoT, ranging from infrastructural considerations like authentication and identity management [Hü15] to diverse application cases, from tourism [Ro10] to agriculture [Wa18]. This contribution presents results of the ENTOURAGE (ENabling Trusted ubiquitOUs AssistancE[4]) project, funded by the German Federal Ministry for Economic Affairs and Energy in the context of the Smart Services World programme, aiming to enable an ecosystem of digital assistants.

2 The ENTOURAGE Ecosystem

From a bird's eye view, the ENTOURAGE project can be structured in three main pillars: technical assistance, interdisciplinary trust, and economic market aspects. The concrete artifacts resulting from the project are: A set of interdisciplinary requirements, laying out basic properties of the ENTOURAGE ecosystem, a coarse-grained architecture, characterizing the building blocks of the ENTOURAGE ecosystem and various types of interconnections between them, a first implementation of the ENTOURAGE ecosystem, enabling a practical evaluation of the aforementioned conceptual artifacts in a realistic setting, and a documented evaluation, including an updated version of the reference architecture.

Work on the evaluation is ongoing, while the requirements, reference architecture, and demonstrator milestones have been successfully passed. This contribution focuses on privacy, security, and identity management functions and architecture of the ENTOURAGE ecosystem. To this end, we will introduce key requirements, definitions, and the ecosystem reference architecture in the following sections. Section 3 will then, after first giving an overview of the preliminary studies, present key ENTOURAGE privacy, security, and identity management functions.

[4] a pseudo-acronym; project homepage: http://www.entourage-projekt.de/

2.1 Definitions

ENTOURAGE focuses specifically on the aforementioned domains of connected mobility and smart home as well as a high density of personal assistants [OL18]. A digital assistant in the sense of ENTOURAGE is an evolution of the smart service concept that is characterized by having the following properties:

Personalization: Assistants leverage knowledge about the user to increase the degree of autonomy they can exercise as well as the usefulness of their functions. This information can be based on user inputs or observations made by assistants.

Context Awareness: Assistants have situational awareness, and can therefore present high-level abstractions to the user, improve the timeliness of their actions, and act autonomously.

Intelligent Interaction: Assistants have multi-modal user interfaces with intelligence such as speech interaction using pattern recognition and natural language processing and graphical user interfaces displaying recommendations.

Proactivity: Assistants can act independently of user inputs, solely based on their context awareness. A typical example for this pattern is system-initiated conversation in a smart speaker.

Network Connection: Assistants are networked with devices, information sources, knowledge bases, classification schemes, and – most prominently within the ENTOURAGE ecosystem – connected to other assistants.

This definition is in line with the one set forth for fuzzy cognitive agents by Miao et al. [Mi07] and for companion systems in the context of DFG SFB/TRR 62 [BW10].

2.2 Requirements

One key result of the ENTOURAGE project is an extensive collection of requirements towards IoT ecosystems, specifically with digital assistants. In this section, we present the key requirements underlying the privacy and security architecture of ENTOURAGE.

Open Market: One key economic aim of ENTOURAGE is to give various vendors the possibility to provide platforms, (personalized) assistants, and assistant components with minimal hurdles of entry and the possibility of differentiation, specifically with regard to security and privacy properties of the assistants. Security and privacy differentiation is limited in that we expect a state of the art baseline from all components of a trustworthy ecosystem, which is enforced by a trust anchor role.

Protocol-agnostic: The concrete underlying network protocols for interoperability of assistants largely dependent on domain (e.g. Bluetooth for in-car integration, ZigBee in the smart home, HTTP for Internet communication), therefore communications security is not in the scope of this contribution. Rather, we focus on the assistants' interfaces. This requirement also entails that there is no prescriptive centralization or decentralization of assistants; specifically, using ENTOURAGE interfaces, it should be possible to connect assistants either directly or via a centralized server.

Platform-independent: One aim of ENTOURAGE is to enable the development of assistants that can then be deployed on various connected platforms as well as assistance components that can then be used by other assistants. Those platforms, assistants, and assistant components may enable varying levels of privacy and security.

Privacy-respecting: Privacy as a basis for trust is a main aim of the ENTOURAGE project. However, as the assistants are personalized, anonymization is not a plausible venue for treatment of the information transmitted in the ecosystem. Therefore, we can derive directly from the standard protection goals for privacy engineering [HJR15] that the focus of privacy technologies on ecosystem level is on transparency and intervenability.

Note that while most infrastructural security aspects are not discussed in this reference architecture, we do encourage individual ecosystem instantiations to aim for a high level of security and investigate unlinkability approaches such as pseudonymization.

2.3 Reference Architecture

A reference architecture captures the architectural essence of similar systems in a domain [Ma15], leaving the details of the software architecture to be filled in for individual instantiations. In the case of ENTOURAGE, this is the domain of IoT ecosystems, more specifically digital assistants. Using a reference architecture brings several benefits that address central ENTOURAGE requirements, most notably improving interoperability of various instantiations (ecosystems), and decreasing development cost—across ecosystems, for several components in one ecosystem, and for new developers [Ma15]. Reference architectures have been successfully applied in many domains, cf. [Ro10].

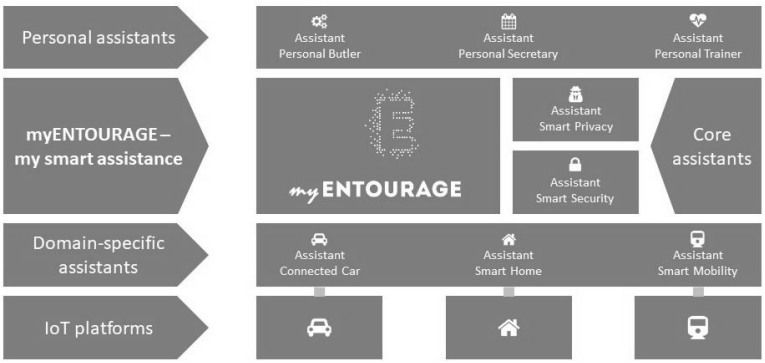

Fig. 1: ENTOURAGE reference architecture

The ENTOURAGE reference architecture is illustrated in Figure 1 and structures assistants into three layers:

Personal Assistants : They have a user interface and get their inputs directly from the user. Personal assistants have no or very limited inbound interfaces for other assistants. They tend to be cross-domain in nature, and tend to have a big amount of knowledge about the user. Examples include speech assistants, time planning/calendar assistants, and personal fitness assistants.

Core Assistants: They provide support functions for infrastructural aspects of the ecosystem, specifically security and privacy. They are linked directly to infrastructural aspects of the communication platform such as access control, information flow filtering, and logging. The functionality of the security and privacy assistants will be described in more detail in Section 3.

Domain-specific Assistants: They are directly linked to a platform. Therefore, they are tend to be domain-specific and have access to a high amount of sensors and actuators. Domain-specific assistants are the main entities that expose interfaces towards the ENTOURAGE ecosystem. Moreover, they are tend to be interconnected, and may specifically be organized in a hierarchical manner.

In addition to these assistant types, the reference architecture contains the various IoT platforms and the myENTOURAGE switchboard. The switchboard links the core assistants to the communication infrastructure which provides further platform independence. It is also the central communication hub in the ENTOURAGE ecosystem, interlinking the various personal and domain-specific assistants. This reduces complexity in highly distributed assistance scenarios. Note that both the assistants and the switchboard can be instantiated with varying feature sets such as differentiation (open market requirement) and can run locally or in the Cloud (protocol- and platform-independence requirements). Particularly, local direct links between assistants can be implemented using stripped down, local instances of an ENTOURAGE switchboard.

The myENTOURAGE switchboard instances are directly linked to a specific user. A user's assistant instances will be registered there. While assistants have several user-specific instances, the knowledge bases of these instances can, but does not have to, be shared. Furthermore, the same instance of an assistant can be linked to several users' switchboards, but will commonly be linked to a specific user.

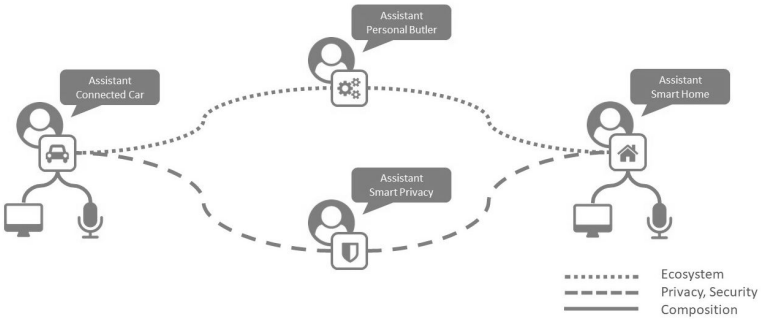

Fig. 2: Interface types in the ENTOURAGE ecosystem

The assistants and platform elements in the ENTOURAGE reference architecture are connected by various communication interfaces (see Figure 2):

Ecosystem Interfaces: They contain high-level functions exposed by the assistants in the ENTOURAGE ecosystem, encapsulating much of the internal state and complexity of the assistant. To leverage synergies with speech assistance interfaces, they may be conversational, or may be similar to state of the art speech assistant interfaces (i. e. HTTP/REST RPC as for Alexa Skills [LQG17]). Due to their high level of abstraction we assume ecosystem interfaces to be understandable to the user, supporting the privacy goal of transparency [HJR15].

Privacy and Security Interfaces: They have the aim of enabling security, transparency, and intervenability [HJR15] for assistants in the ENTOURAGE ecosystem. This includes giving users an overview of their personal information in assistants (being used for e.g. personalization), empowering them to modify this information, and giving users control over learning assistants that is both usable and effective. Those interfaces will be described in more detail in Section 3.

Composition Interfaces: They enable platform-independence by providing standardized interfaces for typical platform functions and components. For example, composition interfaces may be device abstractions or information buses allowing semantic interoperability between arbitrary devices and services. Typically, semantic technologies will be used on this layer [PKP16].

We define an organizational trust anchor as a potential stakeholder of the ENTOURAGE ecosystem, which could continuously ensure an appropriate level of infrastructural security and privacy measures in the platforms, and validate security and privacy claims made by entities in the ecosystem. The trust anchor also provides a contractual framework and certification of ecosystem components.

3 Privacy and Security Assistance in ENTOURAGE

To develop the privacy and security concept of ENTOURAGE, we conducted several user studies. We measured users' preferences regarding transparency and intervenability [ZNH16], and found strong support for automation of functions implementing those protection goals. We also investigated willingness to pay for enhanced security through differentiating encryption [MWZH17], and did not find convincing business models supporting such privacy-enhancements on ecosystem level.

Form the results of our user studies, we can derive two key requirements for the privacy and security concept of ENTOURAGE: First, users want to review and correct their personal information which is used by assistants. Second, users want to have full control of the flow of their personal information. In the following, we describe how the ENTOURAGE privacy and security concept addresses these requirements.

3.1 Privacy

With respect to the first requirement, that users want to review and correct their personal information which is used by assistants, the privacy concept of ENTOURAGE provides two features: First, transparency, which allows users to see an overview of the personal information collected about them by their assistants. Second, intervenability, which allows users to control the collection and processing of their personal information gathered by their assistants. In the following, we describe the implementation of these two features.

Privacy Assistant We developed a privacy assistant that enables users to easily manage their privacy in the ENTOURAGE ecosystem. It provides a *privacy dashboard* and allows users to activate a *privacy mode* at their assistants. The privacy assistant makes use of privacy interfaces to manage the users' privacy throughout their myENTOURAGE instance and assistants.

Privacy Dashboard To realize transparency, we implemented a privacy dashboard. It displays the personal information collected and processed by the users' assistants such as speech commands and locations as well as intermediate results of personalization like

identified points of interest or more general user interests. Moreover, the privacy dashboard provides intervenability by allowing users to delete and correct the personal information collected and processed by their assistants. For an overview of possible architectural variation of privacy dashboards that support various instantiations of the ENTOURAGE reference architecture see [ZAM14].

Privacy Mode To realize intervenability, we implement a privacy mode. It stops assistants from collecting further personal information. While an assistant is in privacy mode, its decisions are solely based on the personal information it collected so far, which might limit the personalized services the assistant provides. No data collecting and learning will be performed based on the observations made in privacy mode.

Privacy Interface We developed a privacy interface to implement transparency and intervenability, or rather, their realization in form of the privacy dashboard and the privacy mode. The privacy interface provides three features: First, retrieval of all personal information collected by an assistant, Second, management of all personal information including deletion, correct, and so forth. Third, de/activation of the privacy mode. The interface is implemented by domain-specific and personal assistants as well as myENTOURAGE and core assistants such as the privacy assistant. The implementation by myENTOURAGE enables a central privacy management. This allows the de/activation of the privacy mode on all assistants through myENTOURAGE, a central logging of assistant communication at myENTOURAGE, and a periodical override of personal information performed by myENTOURAGE on behalf of a user.

3.2 Security

With respect to the second requirement, that users want to have full control of the flow of their personal information, the security concept of ENTOURAGE provides two features: First, a secure authentication with individual credentials. Second a comprehensive authorization system with fine-granular access control capabilities. In the following, we describe the implementation of these two features in ENTOURAGE.

Security Assistant We developed a security assistant which allows users to manage their myENTOURAGE instance. The security assistant is used to register new assistants at the users' myENTOURAGE instance as well as to configure the access control. As the manual configuration of access control rights for each assistant is burdensome for users, the security assistant provides two features: First, it supports trust lists that specific pre-defined access control policies for assistants. Such trust lists can be issued by various organizations such as regulatory authorities and private consumer protection foundations. Users subscribe

to a trust list and when adding new assistants, the access control rights are automatically configured based on the specification of the list. Second, the security assistant provides a wizard [Li16] that asks users a small number of questions to obtain their users' privacy preferences. Based on this information the security assistant preselect the access control rights for assistants.

Authentication Authentication at myENTOURAGE is done by public key cryptography. Each assistant has its own individual key pair and a corresponding certificate which is issued by myENTOURAGE. This enables a strong authentication of each assistant and also enables an individual revocation. Moreover, this solution allows to realize non-repudiation by forcing assistants to sign their messages. This particularly improves the transparency feature (cf. Section 3.1). Fall-back authentication of users can easily be realize by strong passwords [HBB17] and a *universal authentication service* [Hü15].

Authorization Authorization at myENTOURAGE is done by a fine-granular access control system which has two features: First, it allows users to assign general account rights to assistants. Examples for account rights include the right to send message to other assistants through myENTOURAGE and the right to receive a list of all registered assistants. Second, the access control system allows users to assign message exchange rights to assistants. These rights control the flow of personal information between assistants. Examples for message exchange rights include location and time scheduling information. Beside this static control of information flow, the access control system also provides a comprehensive filtering system. It allows to filter the information flow based on the actual content as well as the context of an assistant. Examples include the blocking of information flow while an assistant is in a certain area or sending travel information that contain a certain destination. With this comprehensive access control system myENTOURAGE provides privacy protection mechanisms such as pseudonymization [Ra07], or local processing, filtering, or sanitization of personal information [Da16].

Security Interface We developed a security interface to implement the access control system. It allows the configuration of the account and message exchange rights of assistants at myENTOURAGE. The interface is implemented by myENTOURAGE and core assistants such as the security assistant. Note that the security interface can also be implemented by the privacy assistant. This has the advantage that the privacy assistant has detailed knowledge of the privacy preferences of its users and therefore can configure the account and message exchange rights of assistants more accurate than the security assistant.

4 Conclusion

We presented the security and privacy reference architecture of an ecosystem for digital assistance, building on generic requirements and architectural elements, and also providing more detailed security and privacy patterns. This contribution meets several earlier calls to action from relevant research: Research on privacy architecture is underrepresented in literature [LFH17], as are privacy patterns [LFH17]. Also, digital assistance is a highly relevant use case [LQG17], which is important as finding promising use cases is a well-documented problem for security and privacy technologies, that has been known for an extended period of time [RZ06].

We do not claim the current contribution solves all privacy and security challenges on ecosystem level. We encourage several avenues for future work: Usabile privacy for the IoT remains an interesting field, for example, user consent in complex IoT scenarios is still an open issue [LR13], as are comprehensive transparency mechanisms [To16]. The integration of social, economic, and technology requirements for privacy technologies remains an open issue, e.g., for privacy assistance, which is itself a novel and promising field of research [Li16].

Furthermore, many details of the complex software architecture of an IoT ecosystem are not considered here. This is intentional, as the scope of this paper is a privacy and security reference architecture. It does not mean we do not address these issues. We aim to build on earlier work such as the SkIDentity identity management ecosystem [Hü15], which provides a more detailed architecture and ready-to-use implementations. Another example is a privacy and security architecture for a set of composition interfaces enabling semantic platform interoperability on the IoT that was developed in close cooperation with the BIG IoT project [He16].

The present ENTOURAGE results had significant commercial impact, specifically at consortial partner Bosch, as evident in recent marketing material depicting the ENTOURAGE vision – personal and domain-specific digital IoT assistants interacting to aid the user when interacting with networked devices – in context of the Bosch IoT ecosystem[5]. Furthermore, Bosch is developing various assistance systems – such as kitchen helper Mykie[6] – and generally pursuing an open IoT ecosystem strategy[7].

[5] *„Your Personal Assistant: It's all about you!“* https://www.youtube.com/watch?v=PToWt3itrvA (accessed 2018-08-30)

[6] *„Mykie: Ein persönlicher Assistent für die Küche“* https://www.bsh-group.com/de/newsroom/pressemitteilungen/mykie-ein-persoenlicher-assistent-fuer-die-kueche (accessed 2018-08-30)

[7] *„Ecosystems are the key to succeeding in the IoT. Our IoT platform leverages open source and standards.“* https://www.bosch-si.com/iot-platform/iot-platform/open/iot.html (accessed 2018-08-30)

Bibliography

[Be15] Bercher, Pascal; Richter, Felix; Hörnle, Thilo; Geier, Thomas; Höller, Daniel; Behnke, Gregor; Nothdurft, Florian; Honold, Frank; Minker, Wolfgang; Weber, Michael; Biundo, Susanne: A Planning-Based Assistance System for Setting Up a Home Theater. In: Twenty-Ninth AAAI Conference on Artificial Intelligence. March 2015.

[BW10] Biundo, Susanne; Wendemuth, Andreas: Von kognitiven technischen Systemen zu Companion-Systemen. KI - Künstliche Intelligenz, 24(4):335–339, November 2010.

[Da16] Davies, Nigel; Taft, Nina; Satyanarayanan, Mahadev; Clinch, Sarah; Amos, Brandon: Privacy Mediators: Helping IoT Cross the Chasm. In: Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications. HotMobile '16, ACM, New York, NY, USA, pp. 39–44, 2016.

[HBB17] Horsch, Moritz; Braun, Johannes; Buchmann, Johannes: Password Assistance. In (Fritsch, Lothar; Roßnagel, Heiko; Hühnlein, Detlef, eds): Open Identity Summit 2017. Gesellschaft für Informatik, Bonn, pp. 35–48, 2017.

[He16] Hernández-Serrano, Juan; Muñoz, Jose L.; Bröring, Arne; Esparza, Oscar; Mikkelsen, Lars; Schwarzott, Wolfgang; León, Olga; Zibuschka, Jan: On the Road to Secure and Privacy-Preserving IoT Ecosystems. In: Interoperability and Open-Source Solutions for the Internet of Things. Springer, Cham, pp. 107–122, November 2016.

[HJR15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. In: 2015 IEEE Security and Privacy Workshops (SPW). pp. 159–166, 2015.

[Hü15] Hühnlein, Detlef; Tuengerthal, Max; Wich, Tobias; Hühnlein, Tina; Biallowons, Benedikt: Innovative building blocks for versatile authentication within the SkIDentity service. In: Open Identity Summit 2015. Gesellschaft für Informatik e.V., 2015.

[KGH16] Kubach, Michael; Görwitz, Caterina; Hornung, Gerrit: Non-technical challenges of building ecosystems for trustable smart assistants in the Internet of things: A socioeconomic and legal perspective. In: Open Identity Summit 2016. Gesellschaft für Informatik e.V., 2016.

[LFH17] Lenhard, J.; Fritsch, L.; Herold, S.: A Literature Study on Privacy Patterns Research. In: 2017 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA). pp. 194–201, August 2017.

[Li16] Liu, Bin; Andersen, Mads Schaarup; Schaub, Florian; Almuhimedi, Hazim; Zhang, Shikun (Aerin); Sadeh, Norman; Agarwal, Yuvraj; Acquisti, Alessandro: Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association, Denver, CO, pp. 27–41, 2016.

[LQG17] López, Gustavo; Quesada, Luis; Guerrero, Luis A.: Alexa vs. Siri vs. Cortana vs. Google Assistant: A Comparison of Speech-Based Natural User Interfaces. In: Advances in Human Factors and Systems Interaction. Springer, Cham, pp. 241–250, July 2017.

[LR13] Luger, Ewa; Rodden, Tom: An Informed View on Consent for UbiComp. In: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing. UbiComp '13, ACM, New York, NY, USA, pp. 529–538, 2013.

[Ma15] Martinez-Fernandez, S.; Santos, P. S. Medeiros Dos; Ayala, C. P.; Franch, X.; Travassos, G. H.: Aggregating Empirical Evidence about the Benefits and Drawbacks of Software Reference Architectures. In: 2015 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). pp. 1–10, 2015.

[Mi07] Miao, Chunyan; Yang, Qiang; Fang, Haijing; Goh, Angela: A cognitive approach for agent-based personalized recommendation. Knowledge-Based Systems, 20(4):397–405, May 2007.

[MWZH17] Mihale-Wilson, Cristina; Zibuschka, Jan; Hinz, Oliver: About User Preferences and Willingness to Pay for a Secure and Privacy Protective Ubiquitous Personal Assistant. In: 25th European Conference on Information Systems (ECIS 2017). Guimarães, Portugal, June 2017. Research Paper 3.

[OL18] Olson, Christi; Levy, Jennifer: Transforming marketing with artificial intelligence. Applied Marketing Analytics, 3(4):291–297, 2018.

[PKP16] Palavalli, A.; Karri, D.; Pasupuleti, S.: Semantic Internet of Things. In: 2016 IEEE Tenth International Conference on Semantic Computing (ICSC). pp. 91–95, February 2016.

[Ra07] Radmacher, Mike; Zibuschka, Jan; Scherner, Tobias; Fritsch, Lothar; Rannenberg, Kai: Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen. In: 8. Internationale Tagung Wirtschaftsinformatik 2007 - Band 1. pp. 237–254, 2007.

[Ro10] Roßnagel, Heiko; Zibuschka, Jan; Muntermann, Jan; Scherner, Tobias: Design of a mobile service platform for public events–improving visitor satisfaction and emergency management. In: Joint proceedings of ongoing research and Projects of IFIP EGOV and ePart 2010. Trauner Duck, 2010.

[RZ06] Roßnagel, Heiko; Zibuschka, Jan: Single Sign On mit Signaturen. Datenschutz und Datensicherheit - DuD, 30(12):773–777, 2006.

[To16] Tolmie, Peter; Crabtree, Andy; Rodden, Tom; Colley, James; Luger, Ewa: "This Has to Be the Cats": Personal Data Legibility in Networked Sensing Systems. In: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing. CSCW '16, ACM, New York, NY, USA, pp. 491–502, 2016.

[Wa18] Wagner, Sven; Horch, Andrea; Killian, Bernard; Roßnagel, Heiko: Leichtgewichtige Infrastruktur zur Schaffung von Sicherheit und Vertrauen in einem digitalen Ökosystem für Agrardaten. In: 38. GIL Jahrestagung, Digitale Marktplätze und Plattformen. Gesellschaft für Informatik e.V., Kiel, 2018.

[ZAM14] Zimmermann, C.; Accorsi, R.; Müller, G.: Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy. In: 2014 Ninth International Conference on Availability, Reliability and Security. pp. 152–157, Sept 2014.

[ZNH16] Zibuschka, Jan; Nofer, Michael; Hinz, Oliver: Zahlungsbereitschaft für Datenschutzfunktionen intelligenter Assistenten. In: Multikonferenz Wirtschaftsinformatik 2016. volume III, Universitätsverlag Ilmenau, Ilmenau, pp. 1391–1402, 2016.