# Permission and Privacy Challenges in Alternate-Tenant Smart Spaces

Vitor Jesus [iD] [1,4], Catarina Silva[2],  João Paulo Barraca [iD] [2], Gilad Rosner[3], Antonio Nehme[4], Muhammad Waqas[1], Rui L. Aguiar[2]

**Abstract:** We explore a 'Smart-BnB scenario' whereby someone (an Owner) advertises a smart property on a web platform.  Renters use the platform for short periods, and may fully enjoy the property, including its smart features such as sensors. This scenario should further ensure the Renter's privacy, so we use consent receipts and selective sharing. This paper describes a demonstrator of how smart environments can operate in a privacy respecting manner.

**Keywords:** IoT, Access Control, Permissions, Smart Homes,  consent receipts

## 1      Introduction

With the commoditization of smart technology and communications, shared smart spaces are becoming increasingly common. What was previously "dumb" and "single-feature" devices, such as a simple lightbulb, are now progressively internet-enabled devices that, while delivering basic functionality (such as light) bring with it convenient added-value features. For example, a smart light bulb can have different modes of operation, be controlled remotely with a mobile application, and operations can be scheduled based on the time of the day. A simple lightbulb raises little risk but a lock on a front door or an indoor camera is a different case.

Project CASSIOPEIA (Contextually-Appropriate Selective Sharing IoT Open-standard PErmIssioning Architectures) looks at such scenarios. The setting is a smart home containing a range of devices that are increasingly common for sensing and automation purposes: entertainment systems, environmental sensors, security cameras, etc. Such 'Smart-BnB' scenario, as we call it, we look at dynamic sharing of access to devices inside a smart-space. A Renter books a property for a period in time and an Owner sets access permissions. Such *selective delegation of access* should be simple and effective.

---

[1] PrivDash Ltd, UK – vitor@privdash.com (https://orcid.org/0000-0002-5884-0446), waqas@privdash.com

[2] Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, Aveiro, Portugal: c.alexandracorreia@ua.pt  (https://orcid.org/0000-0002-7969-8813),  jpbarraca@ua.pt  (https://orcid.org/0000-0002-5029-6191), ruilaa@ua.pt (https://orcid.org/0000-0003-0107-6253)

[3] Internet of Things Privacy Forum, Alton, United Kingdom, gilad@iotprivacyforum.org, https://orcid.org/0000-0001-8254-8763

[4] Birmingham City University, School of Computing and Digital Technology, Birmingham, UK – Antonio.Nehme@bcu.ac.uk

Furthermore, devices are expected to collect personal information raising Privacy and Data Protection problems.

This paper shares the challenges and lessons learned by our project during design. In Sect. 2 we describe at the project use-cases. In Sect. 3 we elaborate on key research consideration. Sect. 4, presents our technical approach and Sect. 5 concludes our paper.

# 2    Related Work

The sheer growth in the complexity and volume of global data flows and data processing creates problems with lack of transparency. Users do not, in general, know how their personal data is handled [Ro18] raising Privacy problems, a problem particularly challenging if information crosses boundaries such as between users, systems or countries. In this sense, systems must be designed with base rules centred in privacy while being user-centric. Access control policies must be implemented so the control of personal data relies on the data subject. In several regulations, Consent is the corner stone and under strict conditions – it must be specific, freely given, etc. – so a clear choice is enabled. To this end, Consent receipts is a new consent that promotes choice, ethics and compliance [Je20].

The Internet-of-Things (IoT) poses particular challenges as dataflows are potentially quicker and more personalised collection, including importing domains that were once "offline" or intimate – such as Smart homes [Ji18] . Consent management is a further problem – e.g., lack of screens – which requires a user-centric approach (such as project ADvoCATE [Ra18] or [Mo19]).

# 3    Challenges and Open Questions in SmartBnB scenarios

We briefly highlight some of the challenges a SmartBnB brings.

*Integration of Devices and Identities* – There is no unique agreed interoperability standard, e.g., Zigbee Home Automation, or protocols over WIFI. ONVIF may be an exception, for security cameras, but often low-end devices tend to use proprietary solutions. MQTT provides integration, but mainly for professional solutions. Large Cloud providers are a soft answer offering full stacks. Overall, we observe a highly fragmented landscape. Domoticz, Home Assistant, or Homekit are an alternative path for integration by creating software hubs supporting multiple protocols.

*User Identity* – Identity in IoT is vague and most solutions are centred around a single user. This further implicates Privacy agreements, often tied to IoT vendor cloud infrastructure – e.g., a family camera it blatantly non-compliant when choosing age.

*Delegation of access* – Beyond identity, most devices do not support multi-tenancy,

delegation of access or selective sharing. Parental controls is a common example.

*Consent Receipts* – A Consent Receipt [Je20] records the output of a transaction similar to a conventional shopping receipt. If designed with strong auditability properties, it empowers individuals, make organisations compliant and ethical and allows authorities and watchdogs to effortlessly monitor the market and resolve disputes. There is already a standard [Li17] but perhaps needs improvements for the general case beyond regulations.

*Regulatory questions* – Arguably, the most notable regulation currently is EU/GDPR for which CASSIOPEIA identified interesting questions. Two are the following. First, if our system were run by a company, it would be a Data Controller. Nevertheless, an Owner would also have some control over personal data – a notion of Joint Controller that is not completely clear in GDPR. Second is what happens to consent obtained by the Owner but temporarily delegated to a Renter.

# 4        The CASSIOPEIA Project

CASSIOPEIA investigates how we can create usable and transparent architectures enabling device owners to selectively delegate access to IoT and what happens to personal data collected during different periods. We focus on a smart home that is rented for periods to Renters. Devices collect data with varying levels of privacy and operational impact.

## 4.1        Use-cases

Our overall use-case is described in Figure 1. Before the Renter checks-in, devices are configured by the Owner to give temporary permissions to the Renter. During check-in, the Renter gives consent to collections of their personal data while in the home according to and after reviewing the Privacy Policies of each device.
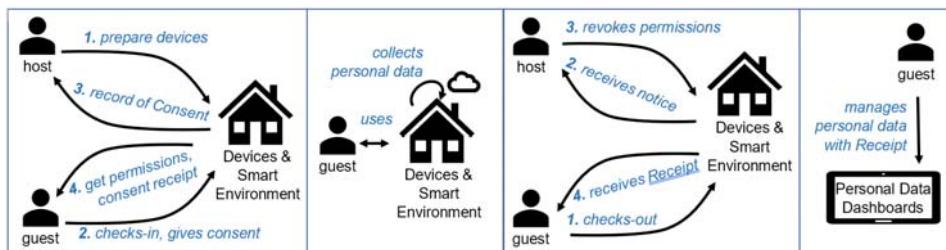


Figure 1: interaction between the host and the renter

During the stay in the Owner's smart home, smart devices collect personal data. The

Owner should not have access to the devices, and even less the data they collect or generate. Exceptions may exist for devices with no impact to the Renter privacy that are important for security purposes (e.g., burglary), or when safety takes precedence (e.g. Smoke alarms). At the end of the stay, and a check-out procedure is actioned, permissions and consent are revoked.

In the final stage, the Renter uses the Consent Receipt to manage any of their residual data collected by the devices. After a retention period, personal data is deleted, and the Renter is notified.

## 4.2    Demonstrator Technical Approach

The project has the secondary objective of creating a publicly available, proof-of-concept demonstrator of the Smart-BnB problem, with real smart devices (e.g., actuators and sensors) to a Smart Home environment. We use "Home Assistant" (https://www.home-assistant.io/) with a lightweight messaging protocol for small sensors.

## 4.3    Demonstrator Technical Approach

Integrations of new smart devices are via Home Assistant; devices include security cameras, SIP doorbells, ONVIF cameras, Zigbee HA and WIFI sensors, smart TVs, etc.

Figure 2 shows the demonstrator architecture. These components offer both the views of an Owner and a Renter. Roles are not supported by Home Assistant so we had to expand the functionality. The *consent manager* is the module where consent receipts are managed and stored. Account management is a dedicated module that enables permissions to be delegated according to roles. Overall, the system architecture enhances user choice, autonomy, participation, and trust. We intend to develop a system capable of *selective sharing* and feature delegation, granular consents, transparency, and non-repudiation.

The permissioning lifecycle is as follows. On the Renter giving consent (and obtaining a Consent Receipt), the Owner delegates permissions that are effective from the check-in date and persist until checkout.

It is essential to guarantee the privacy of the Renter's personal data. During the stay of the Renter, Owners have limited access to devices. On leaving, Renters are able to request erasure of their data, to which the relevant Data Controllers must respond by law. When a Renter leaves the house, the remaining data will be removed. Finally, Renters' access is revoked which concludes the lifecycle. This architecture further prevents current Renters from accessing data of past Renters.
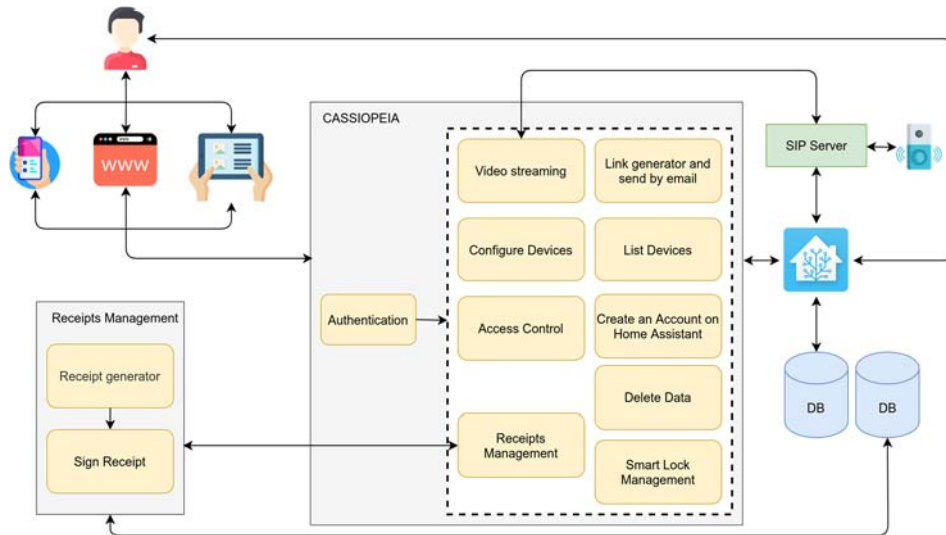
Figure 2: Overarching view of the components of CASSIOPEIA

This component to generate the receipts will be developed as an external service to CASSIOPEIA but will be customised according to the project requirements. The main features of this service will be the generation of the receipt and its control, intermediation of requests between users and data controllers, and the generation of notifications to data controllers.

The structure of the receipt is based on specification by Kantara Initiative but extensively modified to meet our requirements. Initially, a consent receipt is signed and stored on a receipt database. After the authentication on the platform, the user can access his own receipts and personal data associated with them. Personal data is stored in a protected database. Using the platform, the user can manage their receipts and revoke the associated consent while requesting, if wished, deletion of the associated data which, in the absence of a legal reason, must be honoured by the data controller.

## 5       Conclusions and Outlook

In this work, we presented the initial architecture to develop a proof-of-concept demonstrator of the Smart-BnB problem. The use of an open source platform known as Home Assistant, works as a system to collect personal data and the remaining developed systems presented in the architecture serve to guarantee the privacy (between Renter and Owner), receipts generator to manage the receipts and a database to Home Assistant store the personal data and the other database to store the receipts. As future work, we intend to make the prototype publicly available, evaluate its performance and publish the obtained

results.

# 6    Acknowledgement

# 7    Bibliography

[Je20]    Jesus, Vitor. "Towards an Accountable Web of Personal Information: the Web-of-Receipts." IEEE Access 8 (2020): 25383-25394.

[Ji18]    Jiang, Hongbo, et al. "Smart home based on WiFi sensing: A survey." IEEE Access 6 (2018): 13317-13325.

[Li17]    Mark Lizar and David Turner (eds), "Consent Receipt Specification v1.1.0.", Technical report, Kantara Initiative, 2017.

[Mo19]    V. Morel, M. Cunche and D. Le Métayer, "A Generic Information and Consent Framework for the IoT," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 366-373, doi: 10.1109/TrustCom/BigDataSE.2019.00056.

[Ra18]    Rantos, Konstantinos, et al. "ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology." International Conference on Security for Information Technology and Communications. Springer, Cham, 2018.

[Ro18]    Rosner, Gilad, and Erin Kenneally. "Clearly opaque: privacy risks of the Internet of Things." Rosner, Gilad and Kenneally, Erin, Clearly Opaque: Privacy Risks of the Internet of Things (May 1, 2018). IoT Privacy Forum. 2018.