A Trustworthiness-Based Application to Handle Private Data In a FIWARE-Based System

Joao Giao*, Bako Rajaonah†, Elsa Marcelino-Jesus‡ and Joao Sarraipa§
*‡§Centre of Technology and Systems, CTS, UNINOVA, Portugal
†Université Hauts-de-France, LAMIH CNRS 8201, France
Email: jgs@uninova.pt, bako.rajaonah@uphf.fr, jfss@uninova.pt, ej@uninova.pt

***Abstract*—The development of applications to be used on open networks are insecure and provide opportunities for viruses and easy access to confidential information. However, the creation of a trustworthiness layer based solution to handle private data in a FIWARE based system is going to generate an easy to use mechanism to be integrated by applications that have personal information. Creating such secure applications will allow a customized secure infrastructure to validate the user's permission to access the personal information and guarantee the system's integrity.**

I. Introduction

The crescent development of hardware, knowledge and new programing languages is leading to the access of private information across the world wide web, that can be used unethically to acquire monetary goods or privilege information about an entity or person. To reduce these attacks, the applications can apply access rules to define which users are allowed to access the available services and also define which resources they are allowed to use. The solution of this lack of security can be the usage of FIWARE security components that can manage authorization and authentication of one application, the Keyrock and AuthZforce generic enablers together with Enablers Framework, a vf-OS component that makes the orchestration of enablers allows a unique, easy and secure interface to access the enabler's services.

II. The vf-OS Project

The vf-OS (virtual factory Open Operating System) is a collaborative research and innovation project funded by the H2020 Framework Programme of the European Commission under the Grant Agreement number 723710 and conducted in the period of October 2016 until August 2019. It is composed by 14 partners (Users, Technology Providers, Consultants and Research Institutes) from 7 countries with a total budget of approximately 7.5M [1].

The goal of the vf-OS project is to develop an Open Operating System for Virtual Factories (vf-OS), to support a multi-sided market ecosystem for providing a range of services to the connected factory of the future to integrate better manufacturing and logistics processes [2]. The vf-OS is composed by a Virtual Factory System Kernel, a Virtual Factory Application Programming Interface and a Virtual Factory Middleware specifically designed for the factory of the future. An Open Applications Development Kit will be provided to software developers for deploying Manufacturing Smart Applications for industrial users, using the Manufacturing Applications Store at the Virtual Factory Platform [3]. The Virtual Factory Platform is an economical multi-sided market platform with the aim of creating value by enabling interactions between four customer groups: software developers (independent or within individual manufacturers); manufacturing and logistic users; manufacturing and logistics solutions providers; and service providers (vf-OS innovators and third parties).

The Virtual Factory Platform will provide a range of services to the connected factory of the future to integrate better manufacturing and logistics processes. Manufacturing Applications Store will be open to software developers who, using the free Open Applications Development Kit provided, will be able to quickly develop and deploy smart applications to enable and optimise communication and collaboration among supply networks of all manufacturing sectors in all the manufacturing stages and logistic processes [1]. This manufacturing approach can enable a whole new level of flexibility and scalability in the manufacturing domain [2].

An industrial system includes the context, resources, activities, processes, actors, and interdependencies that support the creation and delivery of products and services. A clearer understanding of industrial systems —a holistic view —can identify those 'levers' which are available to generate and, crucially, capture value [4].

During the vf-OS project it was created a framework in order to create a trustworthiness based function handling the data privacy in a FIWARE based system. The EF, represented by Fig. 1, acts as a bridge between service provider and service consumer, providing support for enablers' integration, installation and management of their instances. The EF acts as an aggregator and a common proxy for all enablers that use NGSIv1, NGSIv2, and REST interfaces. To ensure a unique interface and common access for all registered enablers, it acts as a wrapper engine for the different enablers and the vApps. This module represents an advantage for the existing enablers due to the fact that it facilitates the enablers' usage through unique and easy REST API. This EF is composed by the following major sub-components:

Enablers-registry — this module provides necessary functionalities for collecting and persisting configurations and registration details of the framework and integrated enablers. This module also contains the Docker management that allows the administrator user to

	install new enabler's instances
Request-handler	provides a simple interface for vApps to use enablers, known as "Access functionality". It also includes monitoring services that logs performance and Quality of Service (QoS) metrics for both enablers and the framework itself

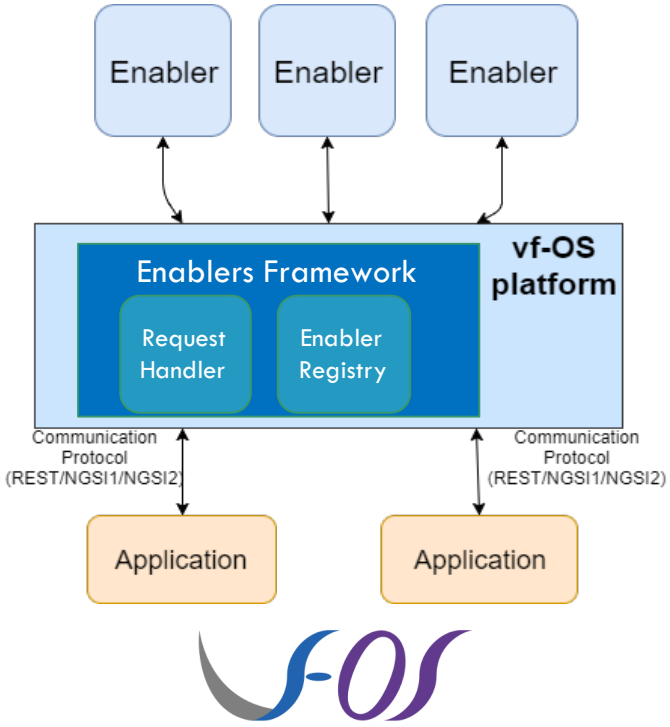

Fig. 1. Enablers Framework - a communication proxy to access the different enablers

FIWARE was a research project with the goal to create a core reference platform in the scope of Future Internet. They currently provide a set of open source software which can be assembled together with other third-party components to accelerate the development of Smart Solutions. These components have been tested and previously included in IoT (Internet of Things) domains such as Smart Cities, Smart Factories or Smart Agriculture [5]. Taking into consideration that these enablers have different access protocols and have specific input parameters, the Enablers' Framework, developed under the vf-OS project, can be used because it aggregates all enabler's information into a single component and works like a proxy, facilitating the usage of enablers. As an example in the vf-OS project, the project is going to use more than seventeen enablers, with different application protocols as well as different services and services' parameters and all these enablers will be accessible through an unique interface and service, allowing the enablers to be interoperable with the remaining modules of the vf-OS environment.

III. Data Privacy in systems as FIWARE

Data privacy refers to personal data, that is, "any information that relates to an identified or identifiable living individual". Recently, the protection of personal data within the European Union (EU) was updated into the new EU General Data Protection Regulation (GDPR) which "regulates the processing by an individual, a company or an organization of personal data relating to on individual in the EU" (see [6],[7]). Data processing means any operation or set of operations performed on personal data such as "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". Clearly, data privacy is a matter of regulation and the organizations who manage users and consumers' personal data have to comply with the GDPR. As emphasized in [8], compliant organizations have a competitive advantage over those that are not compliant. The performance and success of FIWARE-based systems may thus rely on their level of compliance with the GDPR, but to our knowledge scientific literature on data privacy in FIWARE contexts is not still documented, which means that a big work is expected in the future to comply with the GDPR. However, the GDPR is in itself an excellent source of applied research questions. Article 5 of the GDPR recaps the principles relating to personal data processing which are: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. The principle of accountability refers to the demonstration that the principles are applied, which requires controllers (natural persons or legal entities) responsible for attesting the compliance of the personal data processing with the GDPR. Controllers do not process personal data, contrary to the processors (also natural persons or legal entities) who carry out that task on the behalf of controllers. A controller can work alone or jointly with other controllers. However, regarding data privacy handling in FIWARE-based systems, the main issue is neither the potentially exponential number of controllers and processors nor the multiple sources of personal data or their all possible varieties; it is the very open nature of the FIWARE concept with all that it implies: each connectable component that carries personal data should comply with the GDPR.

The Article 35 related with data protection impact assessment (DPIA) is required as soon as the security of natural persons in the terms of their rights and freedoms could be threaten with regard to the processing of their personal data. Personal data breaches may have serious consequences: "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned" ([6], pp.

119/16-17).

Certainly, DPIAs are under the responsibility of controllers, but considering the open nature of the FIWARE concept and thus the multiplicity of responsibilities regarding data privacy management, automatic risk assessments with a systemic approach is necessary, that is, at the global level of the set of socio-technical components which are connected to the platform. A global metric of trustworthiness [9] could be used for such automatic DPIAs, with taking the interdependencies of trustworthinesses [10] in a FIWARE platform into account. Two recent works could serve as a basis for that perspective. First, Geko and Tjoa in [11] have developed and ontology on the interdependence of the GDPR and information security. The second work in [12] has worked on metrics for risk assessment in DPIAs [8] and goes beyond the three criteria of security used in computer science (i.e., confidentiality, integrity, and availability). With regard to one platform that use security components, from a certain threshold of trustworthiness and using a common ontology-based for the GDPR to highlight the requirements for information security, controllers and processors could be triggered if happens a security breach. Both works provide examples of independent security components that are used to orchestrate and control applications related with personal information.

IV. Solution/Discussion

In vf-OS project the Enabler Framework component establishes the bridge between the application and the security components. It is used to register the security services and it allows an unique access interface for the registered services. The architecture represented on Fig. 2 will increase the security by allowing applications to access to the authentication and authorisation security services.

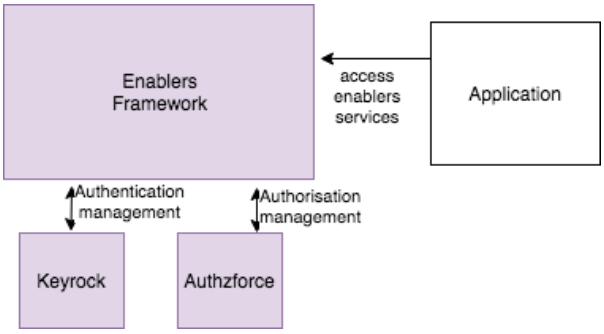

Fig. 2. Interfaces between enablers, EF and application, to manage the authentication and authorisation to access the user's private information

Identity Manager or Keyrock is a generic enabler that is used to administer the authorisation of foreign services to access personal data that is stored in a secure environment. This enabler allows to manage user profiles, enforcement of policies and procedures of user registration, acting as a central component to securely control the users' authorisation of third-party applications [12].

Authzforce is a generic enabler that provides RESTful services to Policy Administration Points (PAP) and Policy Decision Points (PDP) using the OASIS XACML 3.0 standard [13]. The PAP can be used to manage multiple policies and users' permissions rules and PDP can be used to verify whether or not a user request is authorised to access a specific asset, based on the applicable security policies.

The following sub-sections present specific information of the security enablers described above and how the security environment can be configured.

A. Authentication Management

The Authentication component is responsible to verify the authenticity of the user. The application registration into this security component, which should be done by a Security Administrator, uses the following parameters to register one application:

- username: unique identification of the application
- email: email associated with the application. This email can be used to receive private information, such as the identification token or receive a forgoten password
- password: word or string of characters used to prove the identity of the application [13]

The Identity Manager enabler allows the creation of new users with a user interface or through a REST method and use the OAuth 2.0 [14] Framework functionalities, through a OAuth access token. On Fig. 2, the Authentication Management is made with the "Keyrock" module and will be responsible to manage the authentication of the users or applications.

B. Authorisation Management

The Authorisation component, represented by Authzforce on Fig. 2, is responsible for verifying the application permissions. To create these permissions, the Security administrator needs to follow the instructions:

1) Create a security domain. This domain will contain all application's permissions.
2) Create Policy Set Rules. This policy is a XML which contains the parameters that will be used to verify the application's permission.

The policy set rule is a structure which defines what are the resources the application has access to. For this reason, it is very important to correctly define the parameters. On the diagram of Fig. 2, this module will be responsible to store the security policies related with application's authorisations as well as to validate if the application has the required permissions to access specific resources.

C. Data Security Workflow

To use a secure data management, a Security Administrator needs to register the application credentials and define which resources the application has access. The role of a Security

Administrator is important in application such as this one because this security authority has knowledge to correctly and objectively manage, monitor and administrate security over the computer network. These were the instructions used for this paper scenario:

1) Create an application user. The application identification must be unique on the environment to prevent impersonated applications.
2) Get the authorisation token with the previous credentials. This token is used for all the performed tasks the application needs to make, in order to authenticate the application
3) Create security authorisation domain for the application. Specifications of the permissions the application is allowed to access
4) Create the security policies which clearly define the application permissions

D. Enablers Services Requests

In order to use OAuth 2.0 Framework on the application, it is possible to get the authorisation token, through the service "Create token with Token Password method". This Keyrock service requires the application name and password and will return an "X-Subject-Token" that will be used to validate the user identity, as represented by Fig. 3. This figure also demonstrates an example of incorrect credentials, if the application name and password are not correct.

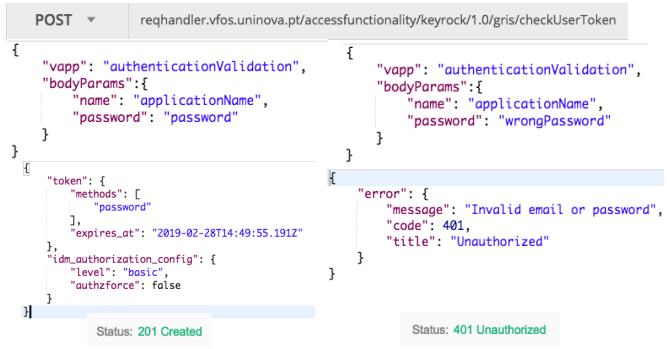

Fig. 3. Authentication management - correct credentials and incorrect credentials. Both examples use the EF to facilitate the requests

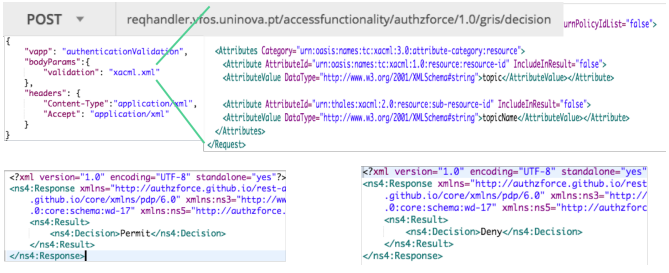

Fig. 4. Authorisation management - the body parameter is an XML and used to verify if the application has permission to access a specific resource, with an accept and reject examples. Both examples use the EF to facilitate the requests

To define the application permissions, the security administrator needs to create security policy rules, through the Authzforce enabler. As mentioned on previous section, these security policy rules are specified using XACML. Fig. 4 is one example of this verification. On the first example the component is allowed to perform an action, and on the second example the component does not have permission to perform an action.

V. Conclusion

Security environments help users and enterprises to ensure that the information they have stored, for example, in a machine or on a cloud, can only be accessed by authorised personnel. The proposed security infrastructure in this paper was designed to use an authorisation and authentication management enabler components and another module, the Enablers Framework, to facilitate and ease their usage. Through the integration of the mentioned components specifically these two FIWARE enablers, developers can protect data by limiting its access and create access rules to prevent abusive data access. Although the focus of this paper is to use this security infrastructure to manage personal data, it can also be used in other domains, such as the manufacturing. It can be used, for example, to manage the factory workers and their accesses in specific factory stations

Specific tests have been conducted in the vf-OS project to validate these interactions. As a future work its intended to use those enablers in the shop floor of the industrial partners of the project.

VI. Future Work

The future work of this interaction between a authorisaton and authentication components through Enablers Framework to secure private information will be applicable on a real industrial environment under the last phase of the vf-OS project - vfStockPolicies - Pilot 1 - Application 3 [15]. The application will be executed in different industrial systems in order to manage spare parts from different manufacturing factories. Since some data must be shared between the factories and another data is sensitive data, the presented interaction from this paper is a crucial security point that will be used to prevent sensitive data to be only accessible for authorised applications as well as prevent the unauthorised access to private information.

Acknowledgment

The research leading to these results has received funding from the European Union H2020 Programs under grant agreements No 611312 vf-OS, as well as from FCT - Fundao para a Cincia e Tecnologia, research unit CTS - Centro de Tecnologia e Sistemas - reference number UID/EEA/00066/2013.

References

[1] Vf-OS consortium, "D8.1a: Validation Scenarios - Vs: 1.0.3," Tech. Rep., 2017.
[2] Vf-OS consortium, "vf-os website." [Online]. Available: http://www.vf-os.eu/about

[3] Vf-OS consortium, “Description of Work of the project ”Virtual Factory Open Operating System (vf-OS)”,” Tech. Rep., 2016.
[4] S. G. FREng, “Industrial Systems: capturing value through manufacturing,” Tech. Rep., 2012.
[5] D. Ferreira, P. Corista, J. Giao, S. Ghimire, J. Sarraipa, and R. Jardim-Goncalves, “Towards smart agriculture using FIWARE enablers,” in *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. IEEE, jun 2017, pp. 1544–1551. [Online]. Available: http://ieeexplore.ieee.org/document/8280066/
[6] European Parliament, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,” in *Official Journal of European Union*, 2016.
[7] European Parliament, “Corrigendum to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46,” in *Official Journal of European Union*, 2016.
[8] H. Li, L. Yu, and W. He, “The Impact of GDPR on Global Technology Development,” *Journal of Global Information Technology Management*, vol. 22, no. 1, pp. 1–6, jan 2019. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186
[9] B. Rajaonah and J. Sarraipa, “Trustworthiness-Based Automatic Function Allocation in Future Humans-Machines Organizations,” in *2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES)*. IEEE, jun 2018, pp. 000 371–000 376. [Online]. Available: https://ieeexplore.ieee.org/document/8523876/
[10] B. Rajaonah, “A view of trust and information system security under the perspective of critical infrastructure protection,” *Ingénierie des systèmes d’information*, vol. 22, no. 1, pp. 109–133, feb 2017. [Online]. Available: https://isi.revuesonline.com/article.jsp?articleId=38019
[11] M. Geko and S. Tjoa, “An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security,” in *Proceedings of the Central European Cybersecurity Conference 2018 on - CECC 2018*. New York, New York, USA: ACM Press, 2018, pp. 1–6. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3277570.3277590
[12] A. C. d. M. Carvalho, “Metrics for Risk Assessment in Data Protection Impact Assessments,” Ph.D. dissertation, Faculdade de Ciênca de Universidade do Porto, Portugal, 2018.
[13] Fiware, “Identity Manager - Keyrock.” [Online]. Available: https://fiware-idm.readthedocs.io
[14] A. Parecki, “OAuth 2.0.” [Online]. Available: https://oauth.net
[15] V.-O. consortium, “D1.3 Providers Scenarios Characterisation - Vs: 1.0.1,” Tech. Rep., 2016.