Ensuring Trustworthiness and Security in Service Compositions

Vasilios Tountopoulos[1(✉)], Ira Giannakoudaki[2], Konstantinos Giannakakis[1], Lefteris Korres[2], and Leonidas Kallipolitis[1]

[1] Athens Technology Center S.A, Halandri, Athens, Greece
{v.tountopoulos,k.giannakakis,l.kallipolitis}@atc.gr
[2] DAEM, Athens, Greece
{i.giannakoudaki,l.korres}@daem.gr

Abstract. Future Internet applications can be dynamically composed of atomic services, which exhibit different trustworthiness and security requirements, when being integrated into complex service chains. In that respect, research in the security field works around solutions that can ensure that security characteristics are well addressed in modern, Web-based, ICT environments, aiming to establish a level of trust and confidence on the service consumers. Towards this direction, this paper showcases the results of the EU-funded FP7 Aniketos project, in order to support the secure development life cycle of Web-based service compositions. It elaborates on the design time and runtime capabilities of the Aniketos platform to support security and trust in the specification of composite service processes, by offering service developers the ability to efficiently express their security requirements and service providers the capability to track security breaches and threats and support decisions on the appropriate mitigation actions.

Keywords: Secure service development · Composition of public services · Trust property

1 Introduction

Secure service composition plays a key role in Future Internet Applications, since the value of the service delivery process increases with the importance of the involved data and their security requirements. Different types of multi-source information are integrated into distributed ICT platforms and services to facilitate the needs of multiple cross discipline business domains, which require the composition of public and private service processes. However, the integration of any type of data in complex service provisioning paradigms raises valid concerns on the security and privacy vulnerabilities of data systems to maintain the value of the offered information content [1].

As a consequence, end users appear to be reluctant in using such ICT systems and they expect to increase their perceived confidence by setting specific trust and security requirements that should be met. In this context, this paper approaches the problem of security by design to support the development and execution of data driven composite

F. Cleary and M. Felici (Eds.): CSP Forum 2014, CCIS 470, pp. 3–15, 2014.
DOI: 10.1007/978-3-319-12574-9_1

services, which are consumed in critical business domains to build secure Web-based applications.

The paper presents the results of the FP7 Aniketos project [2] to address the problem of the design time support of security properties in the provision of sensitive data in composite service processes, with application to a variety of business sectors. More specifically, it demonstrates how specific end user security and trust requirements are evolving to system level security mechanisms to deliver complex interactive Web service-based applications that require the integration of critical information, which is subject to various security classifications.

In a nutshell, the scope of the paper is to present the applicability of the research work conducted in the context of the Aniketos project on domain specific application scenarios, which raise certain security concerns that have to be effectively addressed in the design, development, deployment and execution of secure composite services. In that respect, the paper is structured as follows: Sect. 2 gives an overview of the technical aspects of the Aniketos project and, presents the Aniketos methodology for developing secure composite service specifications and integrating them in operational and highly business-oriented Web applications. Then, Sect. 3 introduces the software packages comprising the Aniketos platform, which is the main outcome of the Aniketos project by providing software level implementation details. Then, Sect. 4 elaborates on how the platform has been used to develop secure composite services in the context of an e-Government application, which exhibits certain security and trust requirements. This section, also, introduces the main results collected as feedback from the evaluation of the Aniketos design time and runtime capabilities. Finally, Sect. 5 concludes this paper.

2 Overview of the Aniketos Project

This section makes an introduction to the objectives of the Aniketos platform and introduces the technical directions, towards which the Aniketos work delivers significant results to advance the current state-of-the-art in the area of secure service engineering. This section, also, presents the methodology that is adopted to realise the Aniketos research in real application scenarios.

2.1 Introduction to the Project Objectives

The main objective of the Aniketos Project is to establish and maintain security and trustworthiness in composite services. The project delivers a platform that builds upon existing environment solutions, such as service composition, service runtime execution and service storage, and extends them to offer the security and trust dimension when designing, implementing, deploying and running composite services.

In more details, the Aniketos platform aims to advance the state-of-the-art in the area of service composition by creating and maintaining secure and trusted composite services. Through the appropriate specification of methods and development of tools and services, the Aniketos platform supports the whole service life cycle in service

engineering, ranging from service implementation, discovery and composition to service management, adaptation and reconfiguration.

As Future Internet services can be dynamically composed or evolved, the Aniketos platform defines trust models and security policies, through which the interested stakeholders can define, validate and monitor trustworthiness and security properties. These properties can be used as the building blocks for developing the security descriptors for the composed services and contract related artefacts, as well as be exploited to identify and overcome the shortcomings in service engineering when dealing with security violation issues.

Security violations can occur when systems and services are vulnerable to intruders, which may affect the set security standards and the quality of experience received by the users. Towards this direction, the Aniketos platform tries to address potential loss on service availability and end user trust by efficiently analysing, solving and sharing information on how new threats and vulnerabilities can affect service compositions and can be mitigated [3], so that the composed services can be (semi-) automatically adapted to the new runtime conditions.

On top of that, the Aniketos platform adds a socio-technical perspective to the way that security and trustworthiness requirements are addressed in service engineering. Since service and service-based systems target highly business-oriented environments, the respective business processes, which are being supported through the deployment of the appropriate composite services, are governed from both technical and social aspects. Such aspects should be tackled together once security and trust are considered.

2.2 The Aniketos Methodology

The adoption of the Aniketos concepts is based on existing secure software development methodologies. Our approach extends them to provide the roadmap on how the innovative technologies of the Aniketos platform can be integrated in order to advance compositions of data critical services to be more secure, reliable and trusted.

As data driven future Internet services can be dynamically composed or evolved, the Aniketos platform gives emphasis on the definition of both human readable and machine readable security policies, through which the involved stakeholders in a service chain can validate the offered security properties and monitor the trustworthiness of the associated providers. These properties affect the availability of sensitive data and can be used for the implementation of the security descriptors of the composed services and contract related artefacts, as well as be exploited to identify and overcome the shortcomings in service engineering when dealing with security violation issues at runtime.

More specifically, the Aniketos platform capabilities are realized through three distinct phases, as depicted in Fig. 1. As a first step, we show how the Aniketos platform relates to the secure service development of data driven composite services and applications by enabling domain security experts and service designers and developers in the design-time service process specifications taking into account security and trust requirements [4, 5]. The requirements are expressed in the form of security consumer policies with respect to how data is provided and shared among participating data holders and consumers.

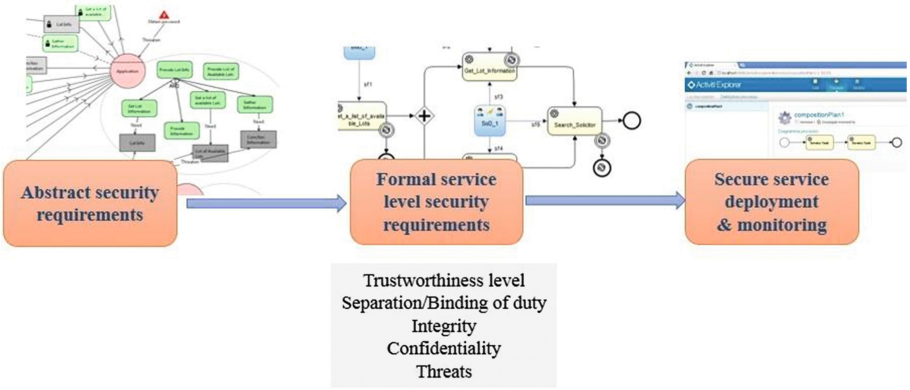

Fig. 1. The methodology for the use of the Aniketos platform

The requirements can be described in a high level XML like specification language, which can, then, be mapped to a formal service specification language, like Business Process Modelling and Notation (BPMN) [6]. Based on the defined security policies, the Aniketos design time methodology prompts service developers in linking service processes with actual atomic services, which satisfy these policies. Thus, the composition of the service process chain is verified on the security assertions that the target service consumers have declared as requirements [7]. The development of the secure service compositions is based on the Activiti Modeler[1].

At runtime, the designed specification of the secure service composition is deployed, so that it can be exploited in domain specific application development. During the announcement phase, the service developer can define a set of rules to accompany the service contract and which can potential drive the runtime behaviour of the service execution, in order to handle security violations and threat exposures. The deployment and execution of the composite service specifications is performed through the Activiti Engine (see Footnote 1). As a last step of our approach, the Aniketos platform enables monitoring of the runtime execution for the relevant composite services to ensure that the provisions of the security contract are respected and that the potential exposure of threats is well addressed [8]. In case of violations, the platform enacts automatic service adaptation mechanisms, through re-composition or re-configuration.

3 The Offerings of the Aniketos Platform

The Aniketos platform has followed a modular approach for the architectural design, which enables the platform to be installed either as a platform as a whole or as separate components. This gives the target users the advantage to choose the functionalities that they want to install.

[1] http://www.activiti.org

The Aniketos Platform and Environment components have been grouped to software packages, which better facilitate the delivery of the Aniketos platform functionalities to the target user groups. The platform architecture has been based on the OSGi framework[2], which is a standardised technology, fully documented, that defines a dynamic modular system for Java applications [9, 10].

Thus, here we introduce the potentials for grouping the Aniketos provisions into software packages, which can be commercialised directly to the target markets and facilitate real life needs for supporting security and trustworthiness in a variety of (cross-discipline) application domains. The packaging takes into account the details of the components, their licensing scheme and their position in the Aniketos methodology presented above, including the security service development lifecycle.

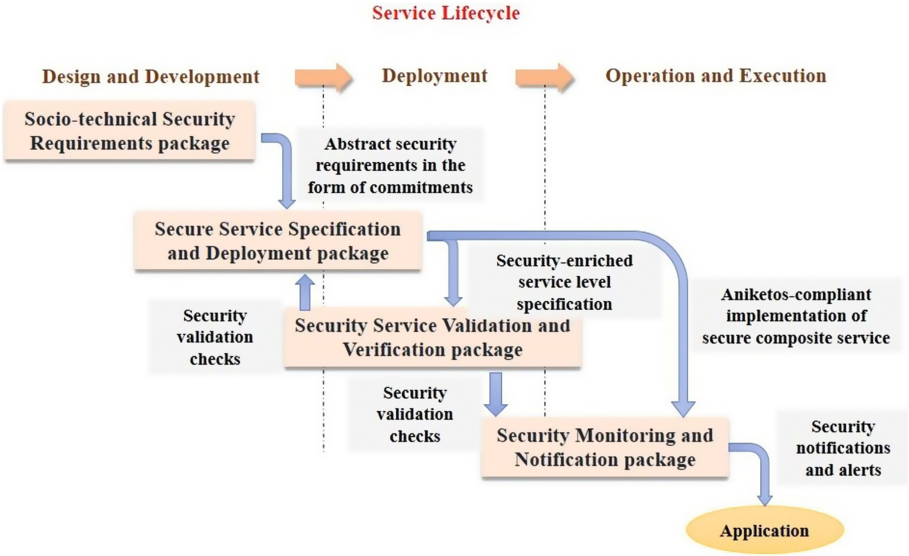

Fig. 2. The software packages of the Aniketos platform

As shown in Fig. 2, the Aniketos platform is provided as four distinct software packages, which are summarised in the following lines.

The Socio-technical Security (STS) Requirements package offers the ability to model the security requirements in complex services [11]. The language and tools allow us to represent the agents and the roles involved in the service execution, the goals they should achieve, the trust and security relationships among them, and the documents specifying the achievement of these goals. This package generates security requirements for services, whether they are developed from scratch or already exist and need to conform to certain security rules and organisational policies. By using this package, we can involve different stakeholders and specify our security requirements

[2] OSGi Alliance Specifications - http://www.osgi.org/Specifications/HomePage.

by exploiting close to real world modelling practices. This package facilitates the design phase of the Aniketos security lifecycle.

The Secure Service Specification and Deployment package enables business process modelling of composite services and configuration of the security requirements, which can be retrieved from the previous package or defined from scratch. The package allows easy deployment of the composite services in a runtime environment. For each service part, the functional specification is enriched with security characteristics, detailing the level of security that should be supported [12]. The package offers the possibility to publish services to a service registry and supports searching in this registry to discover the most appropriate atomic services to be associated with the composite service. This package facilitates both the development and deployment phases of the Aniketos security lifecycle.

The Security Service Validation and Verification package checks the design, registration and execution of secure service specifications. When a composite service has been designed, the service developer needs to check the security characteristics of the constituent parts involved in the service composition. These verification checks are performed at runtime to validate that the composite services maintain their security properties and comply with security policies at execution time. This package comes across the Aniketos security lifecycle and can cover all the involved phases.

Finally, the Security Monitoring and Notification package enables monitoring of the execution of secure composite services and generates alerts when any malfunctions are identified. Such malfunctions can refer to the violation of a service contract, the degradation in the trustworthiness, and the threat level of the offered composite service or parts of it. The package supports subscriptions to service monitors for specific types of events. It monitors events in the service execution environment and analyses them in order to generate alerts and notifications about potential breaches to security and trustworthiness requirements. This package facilitates both the deployment and execution phases of the Aniketos security lifecycle.

The four software packages of the Aniketos project results are available in both basic, open source versions[3] and closed source providing additional and more advanced functionalities, especially in the field of security verification checks. Through these packages, the Aniketos platform offers design time and runtime support of security and trustworthiness properties in the provision of composite services. More details about the Aniketos software packages can be found in [2].

The platform capabilities address the needs of different stakeholders, including service and application developers and service providers. The service developers can exploit the Aniketos platform at design time to define trustworthiness and risk-based security properties over and between external service components. By adopting the Aniketos design time methodologies and tools, as presented above, they are able to create composite secure service specifications, discover and select the most appropriate secure service components and evaluate the compliance of service compositions with respect to set security user requirements and service properties.

[3] Available at github.com/AniketosEU.

At runtime, the Aniketos platform offers software packages, which enable the service providers to publish their composite service specifications and operate their secure and trusted services, and application developers to monitor the operational behaviour of composite service executions and efficiently react in cases of contextual environmental changes and security violations. Thus, when changes occur that have an impact in the proper and secure service execution, the Aniketos packaged platform is notified to take the appropriate actions and potentially proceed with service recomposition and reconfiguration, according to the best service adaptation potential.

4 Building Secure Service-Based Applications

This section describes the way that the Aniketos platform is used to develop secure composite services that can be consumed in business-oriented applications. The section introduces the steps that should be adopted by the involved service designers, developers and providers during the whole service lifecycle. This section is concluded with some initial remarks arising from the evaluation of the Aniketos platform through the realisation of a use case facilitating the needs of an e-Government scenario.

4.1 Development of a Use Case Application

In the scope of this paper, we exploit the capabilities of the Aniketos platform to showcase their applicability in real life examples and evaluate the practicality of the platform functionalities in commercially critical environments. For our case, we select an example from the e-Government regime, which constitutes a demanding case of public and confidential information being integrated into a secure service based application. This example aims to address the citizens' security concerns when participating in e-Government online public services following a security-by-design implementation approach.

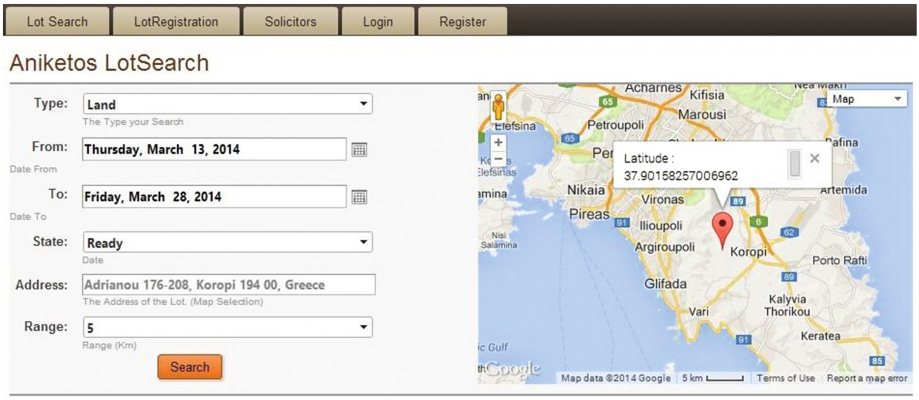

Fig. 3. A screenshot of the Web application for the e-Government domain

More specifically, in order to evaluate the Aniketos methodology towards supporting the design time specification of secure service compositions and the deployment of Aniketos compliant composite services, we have used the Aniketos platform to develop a set of composite services that have been consumed in this e-Government Web application, facilitating the task for publishing the lot information residing in a given area (see Fig. 3 for the end user view of this application). The development process has been made aiming to evaluate the capability of the platform to provide the necessary level of abstraction and enable (not necessarily security skilled) service designers and developers define their security and trustworthiness requirements in the specification of complex public services.

The functionalities that have been exposed by the platform and have been used to develop this e-Government application are analysed in the following steps, which implement the Aniketos approach to build secure service-based business applications:

- Build security requirements-based service specification for publishing lot information scenario: an initial structure of the Aniketos compliant specification is built, based on abstract security requirements (see Fig. 4), being defined through the STS package, and after their transformation to concrete service specification resources.
- Define security policies for the publishing lot information service tasks: the Aniketos compliant specification is enriched with more security requirements at the level of the formal service specification.
- Create candidate compositions by discovering existing services to facilitate the publishing lot information process: the tasks associated to a composite service specification are linked to actual service components, which are discovered from the Marketplace, based on functional and security characteristics.
- Analyse service properties: the Marketplace requests for the validation of the security properties of a service with certain functional characteristics.
- Perform design time service verification: the list of candidate service specifications are verified to ensure compliance of service security properties with defined consumer policies.
- Deploy the Aniketos compliant service specification for the publishing lot information process: the most suitable secure service specification is selected for deployment to the runtime platform and the subscription to monitoring services is performed. Alternative secure service specifications are stored for runtime reference and use.
- Announce the publishing lot information secure composite service: the deployed service specification is checked with respect to claimed security properties, prior to the announcement to the Marketplace, as an Aniketos compliant service specification.
- Subscribe to notifications: the deployed service specification registers to the Notification services of the Aniketos platform to receive alerts in cases of events, such as (a) contract changes, (b) trust level changes, (c) threat level changes and (d) any other contextual change of the functional and security characteristics of the services.
- Monitor the execution of the service with respect to the publishing lot information: monitor the execution of the Aniketos compliant service to identify changes in the proper runtime behaviour, based on the Agreement Template.

- Perform runtime service verification: in case of any violations, the properties of the composite service are verified at runtime to identify the type of violation and provide reasoning over the appropriate actions to be followed.
- Invoke service re-composition to maintain the security and trust policies for the publishing lot information process: the necessary actions towards re-composition of the runtime behaviour of the service are performed. The execution of the service is not interrupted.
- In case that re-composition fails, invoke service re-configuration: the necessary actions towards re-configuration of the composite service specification for the publishing lot information process are performed. The execution of the service may be interrupted.

Based on these steps, we have managed to develop a composite service specification, as shown in Fig. 5, which facilitates the publishing lot information scenario,

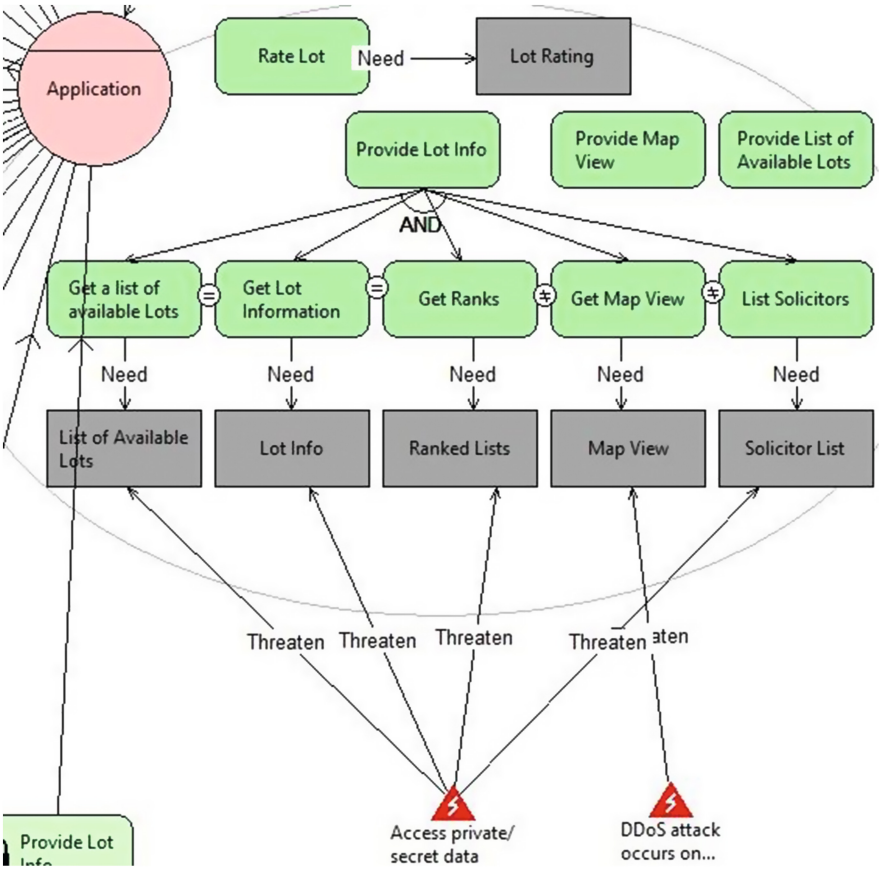

Fig. 4. An extract of the security requirements-based specification for the publishing lot information composite process

with a set of given security and trust properties applied to it. This composite service process has been consumed in a Web-based application, to offer the runtime realisation of the execution level capabilities of the Aniketos platform.

In order to facilitate the proper operation of the Web application through the Aniketos platform, we have performed different test scenarios at runtime, which include the conduction of various trigger events to form and emulate a violation of the specified security agreement. Thus, the application is tested to observe the runtime behavior for different configurations of the service execution, aiming to showcase how and when service re-composition and reconfiguration occurs, in accordance to the specific runtime rules.

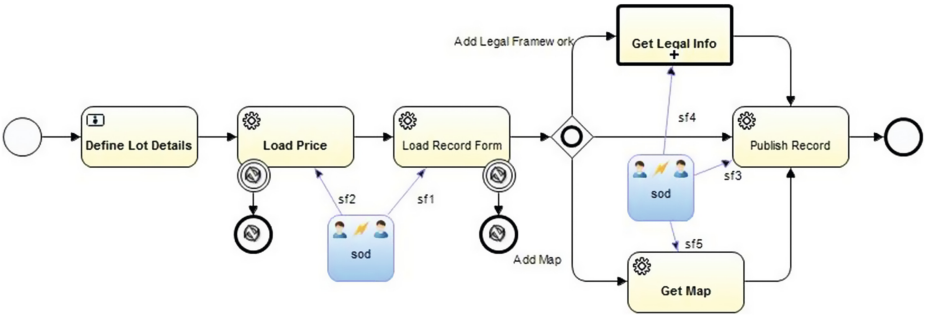

Fig. 5. The service specification for the publishing lot information composite process

4.2 Evaluation of the Aniketos Platform Through This Business Application

The evaluation of the Aniketos platform has been based on the scenario specific development process, described in the previous section. The evaluation process has been evolved through both focus group discussions and structured feedback in the form of questionnaires. The overall result of the evaluation shows that the use of the Aniketos platform in real life applications is very useful for the designers, developers and domain experts in general, since it supports them to define security needs at various levels and navigate through the actual service process, hiding the complexity of the secure service design and deployment tasks.

In a group of highly relevant stakeholders, we demonstrated the Aniketos methodology to build the application for the publication of lot information. During the demonstration and in the discussion phase after it, specific advantages and disadvantages regarding the usefulness of the Aniketos capabilities were discussed, while issues with respect to future extensions were raised. A very useful overall outcome for the Aniketos platform is the seamless integration from the design time to the deployment of secure composite service specifications, which can, then, be reused in the context of another composition and, subsequently, be consumed in another application.

Furthermore, the specification of security requirements in a collaborative manner, in which you have different stakeholders sitting together in order to define the complex

process is another asset for the Aniketos platform and the level of expertise from the these stakeholders that needs to be captured in the platform. This, also, drives how security is applied as part of the high level concept of the application, which is, then, mapped to specific service processes with certain security restrictions.

Despite the positive points raised in the evaluation feedback, some missing aspects have been spotted down as well. Of particular interest for future work is the fact that the evaluators would like to see the whole set of security properties that you define at the design phase to be populated after the deployment phase as well. Emphasizing on the security properties lifecycle, it would be of great importance for the service providers to be able to visually track the evolution of the security property values at runtime. For example, if you specify a trustworthiness level during the development of a service composition to be greater than 0.5, you should be able to monitor whether the provided services offer a trustworthiness level greater than 0.7 or not.

Another important feature that has been suggested during the evaluation refers to the ranking of the available candidate compositions at the development phase. One should be able to balance the algorithm of the ranking, by giving specific weights over, for example, the trustworthiness and the credibility criteria, resulting to a hybrid ranking experience. This might be useful when you have different security requirements along your process and the service designer should be able to define the balance on the ranking across these security requirements.

As an overall evaluation statement, using the Aniketos platform, it turns that service composition can be enhanced, enabling the involved stakeholders establishing a sense of trust when using the respective software packages. In the e-Government domain, service composition is subject to security restrictions and concerns, which are potentially driven by legal limitations. Thus, in this specific domain, in which citizens and enterprises' trust on ICT systems owned by the local authorities lowers with the credibility of the public bodies, the need for a third party "certification" of best practice development is necessary. The same is applicable to an extended list of paradigms in various business sectors, in which the exploitation of the Aniketos platform provisions can eventually minimize the final costs for developing future Internet applications, paying specific attention to security concerns existing in them.

5 Conclusions

Today's ICT systems are evolved within a service-based space, in which data plays a key role as a valuable asset of the service engineering process. Web content is continuously made available and is being provided through Web services, which are autonomously or synergistically operate to feed the business execution of any kind of organisation, including commercial branches, industries, and governments. As the value the involved data streams increases, the need for protecting the composition of the service delivery processes is increased as well, aiming to offer innovative services for the consumers of Future Internet applications and systems.

In this paper, we presented the security by design concepts built in the Aniketos project, when developing composite services, focusing on an example from the public service delivery domain. We elaborated on the Aniketos methodology to deliver

security solutions that are bound to the actual needs of the service development lifecycle, in which service developers can express specific high level security requirements and translate them to service process level requirements, which are associated with the secure service specifications being constructed in a formal language (namely secure BPMN).

By defining own security policies, service developers can investigate on the appropriate combination of atomic services in a composite service process chain and enact the execution of the composite service process to monitor that at runtime the specified security attributes are compliant to the expressed security policies. In that respect, the paper offered realisation on how the development and deployment of Aniketos compliant composite services in the context of business level applications, and in our case for the e-Government domain, can be affected by the security provisions of individual service components.

At this point, we would like to mention that this work is partially funded by the European Commission under the FP7 Framework Programme and Grant Agreement 257930 Aniketos project [2]. We would like to thank all Aniketos partners in contributing to the design, specification, development and evaluation of the Aniketos capabilities and the delivery of the Aniketos platform, which was the basis for the work in this paper.

References

1. Meland, P.H., Guerenabarrena, J.B., Llewellyn-Jones, D.: The challenges of secure and trustworthy service composition in the Future Internet. In: 2011 6th International Conference on Proceeding of System of Systems Engineering (SoSE). IEEE Computer Society (2011)
2. FP7-257930 Aniketos project. www.aniketos.eu
3. Georgia Institute of Technology, "Emerging Cyber Threats Report 2014". Georgia Tech Cyber Security Summit 2013
4. Pajaa, E., Choprab, A.K., Giorgini, P.: Trust-based specification of sociotechnical systems. Data Knowl. Eng. **87**, 339–353 (2013). doi:10.1016/j.datak.2012.12.005. Elsevier
5. Paja, E., Dalpiaz, F., Giorgini, P.: Managing security requirements conflicts in sociotechnical systems. In: Ng, W., Storey, V.C., Trujillo, J.C. (eds.) ER 2013. LNCS, vol. 8217, pp. 270–283. Springer, Heidelberg (2013)
6. Object Management Group(OMG), Business Process Modelling and Notation (BPMN) specification v2.0, January 2011. www.bpmn.org
7. Brucker, A.D., Malmignati, F., Merabti, M., Qi, S., Bo, Z.: A Framework for Secure Service Composition. In: Proceedings of the International Conference on Social Computing 2013 (SocialCom), IEEE, pp. 647–652, doi:10.1109/SocialCom.2013.97
8. Ayed, D., Asim, M., Llewellyn-Jones, D.: An event processing approach for threats monitoring of service compositions. In: Proceedings of the 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS), IEEE, pp. 1–10, doi:10.1109/CRiSIS.2013.6766363
9. Hall, R.S., Pauls, K., McCulloch, S., Savage, D.: OSGi in Action. Manning Publications Co., Greenwich (2011)
10. Cummins, H., Ward, T.: Enterprise OSGi in Action. Manning Publications Co., Birmingham (2013)

11. Dalpiaz, F., Paja, E., Giorgini, P.: Security requirements engineering via commitments. In: Proceedings of STAST'11, pp. 1–8 (2011)
12. Brucker, A.D.: Integrating security aspects into business process models. IT Inf. Technol. **55** (6), 239–246 (2013). ISSN: 2196-7032. doi:10.1524/itit.2013.2004. http://www.brucker.ch/bibliography/abstract/brucker-securebpmn-2013. Special Issue on Security in Business Processes