Workflow Operational Assurance for Security-by-design Certified Service-based Coalitions

Javier Espinar, Antonio Maña, Hristo Koshutanski
Departamento de Lenguajes y Ciencias de la Computación
Universidad de Malaga
Malaga, Spain
espinar@lcc.uma.es, amg@lcc.uma.es, hristo@lcc.uma.es

Abstract— *The concept of Dynamic Coalitions (DCs) provides a scalable approach for service-based business integration suitable to Small and Medium-size Enterprises (SMEs). An outcome of a DC model is a composite service offered to a market place. The notion of security-by-design certified coalition enables coalition designers/owners to request a certification authority to certify whether the coalition workflow design supports certain security properties of interest by stipulating the security properties individual services have to conform to. This paper presents an approach based on a novel Highly Dynamic Coalition (HDC) concept able to provide workflow operation assurance for security-by-design certified service-based coalitions. Certified HDC models can become an enabler for SMEs to participate in coalition formations guaranteeing a certified level of security. Users of HDC-based services will have assurance for the properties preserved during coalition operation, while service providers will have assurance in providing services during HDC formations and partners' selection phases. We will show how workflow operation assurance is realized by means of service security certificates developed in ASSERT4SOA project.*

Keywords—*Workflow security assurance; highly dynamic coalitions; security-by-design certified coalition; service security certificate.*

I. INTRODUCTION

Dynamic coalitions (DCs) consist of independent organizations that share resources and skills to achieve significant mission objectives. These types of coalitions allow small and medium-sized enterprises (SMEs) to be more innovative and competitive in the market, adapting to new opportunities in a dynamic business environment. We have defined *highly dynamic coalitions* (HDCs) as a subclass of DCs in which coalition formation and operation processes are strictly bound by time and performed through automatic means in order to provide a prompt reaction to some events [1,5]. HDCs are defined as abstract workflow models, which are instantiated dynamically, on-the-fly by selecting specific partners for the composite services of a coalition. In the proposed model, organizations (SMEs) register to a coalition platform and select which HDC models they wish to participate in, which services they are wiling to provide, and what business roles to play. Partners registered to an HDC model are automatically selected when an HDC instance is generated, based on some business, quality, and security criteria, and become active participants from the time the coalition is formed. HDC instances are formed in response to a specific request e.g., a market demand, business opportunity, or disaster response, to name a few.

In such service-provisioning model, the coalition owner has no longer full control over the provided services. This lack of control, especially in critical domains such as financial, defense and healthcare, raises concerns about the security of these services [2]. Pre-established trust relations between coalition owners and service providers, such as Service-Level Agreements (SLAs), traditionally represent mitigation to this situation. However, they can be hardly established in a dynamic and scalable manner that would fit in HDC environment where new and cost-attractive offerings from different service providers are frequently launched. Given such a dynamic collaborative environment, guaranteeing security assurance of a coalition workflow model becomes of utmost importance since partners participating in a coalition will likely have heterogeneous security models for service provisioning. Assuring overall coalition security properties during coalition formation and operation phases are of major concern to both the users of coalition services and providers of those services.

The notion of security-by-design certified coalitions allows coalition designers (or owners) to request a certification authority to certify whether the coalition workflow design supports certain security properties of interest and what security properties individual services have to conform to. In that way, global coalition security properties are certified in accordance to stipulated security properties of individual services that have to be guaranteed during coalition lifecycle.

HDC workflow models can be certified based on design-time analysis on the workflow model, and relevant certification criteria and techniques to reason on security aspects in service composition. Certified HDC models will be source of assurance and enablers for SMEs to participate in coalition formations with a given level of security assured by the certified security properties.

Paper contribution. The paper presents a platform-driven approach able to realize the concept of HDC and guarantee the security-by-design certified coalition properties during coalition life cycle, especially during automated coalition formation and operation. It is presented how the workflow security assurance is realized by means of service security certificates developed in ASSERT4SOA project.

The paper is structured as following. Section II presents a scenario illustrating the need of security assurance in dynamic coalitions. Section III discusses related work. Section IV presents a conceptual model of the HDC security assurance and introduces the platform approach. Section V presents a platform-driven HDC lifecycle, while Section VI presents the enhanced lifecycle for security assurance. Section VII recalls the scenario but with concrete example of security properties. Section VIII concludes the paper and outlines future work.

II. Scenario

We will present a (simplified) stock brokerage scenario, to illustrate the functionality of the HDC concept for business aggregation, and will motivate the need of security-by-design certified coalition in order to provide assurance for service providers and users of the stock brokerage service.

A stock brokering company BROKCO provides services to end users, stock investors, by means of its own web-based application. However, BROKCO relies on services provided by external specialized companies in order to compute and recommend the best portfolio for clients' investment requests. Currently the composition and orchestration is static and has been done manually. However, BROKCO knows there are several providers for the same services, each one with their own advantages and limitations, and would like to be able to dynamically choose the providers' services depending on end-user needs and security properties of services.

To carry out the new scenario, a HDC workflow model is defined with the abstract services described below so that the external specialized companies will register to this HDC model as providers for the corresponding services they offer.

- *Stock Service (Stock)* provides information about the current values of the stock and the predicted values of the stock based on the requests it receives,
- *Payment Gateway Service (PayGat)* processes a payment transaction on behalf of a stock broker,
- *Stock Exchange Service (Exch)* allows a stock broker to purchase the stocks on behalf of a stock investor,
- *Storage Service (Store)* allows a stock broker to store reports of each transaction.

In order to determine the ideal portfolio for the client and to complete the investment process in the name of the client, BROKCO needs to select dynamically, at user request time, the most appropriate service providers according to the specific request received from a client. This is precisely the need to have an automated coalition formation per user request in order to guarantee the most optimal partner selection for the user's portfolio (i.e., maximizing client benefits and fulfilling client restrictions and preferences).

One of the major responsibilities that BROKCO has to face is to protect the personal user data and secure the investment data throughout the entire HDC workflow. Given that BROCKO does not have control over the entire workflow process because several external to BROCKO Web services are called, and several assurance issues arise on whether security- and privacy-related aspects are preserved not only on the BROCKO's side but also on the side of services as provided by the specialized companies.

In order to provide assurance to users on the protection of user personal data for the entire workflow model (as requited by national legislation), BROCKO requests security certification to an accredited authority for the BROKCO composite service, to (formally and legally) express security properties the BROCKO service (workflow) supports and the security properties the individual abstract services have to preserve. The outcome of the certification process is a digital certificate expressing the security properties of the BROCKO service (the HDC workflow) conditioned by the security properties each involved service must preserve.

The main goal of the HDC model is to dynamically select providers' services that comply with the functional and non-functional requirements including the required security properties. To achieve these objectives the paper proses a platform-driven approach able to realize the HDC workflow operational model by assuring the certified security properties are preserved during coalition lifecycle.

III. Related work

We will overview related work with a focus on how coalition-level assurance could be addressed.

A. *Authorization-driven Assurance for Cross-organizational Resource Sharing*

There are several approaches applying semantics to enhance authorization interoperation across heterogeneous systems. Warner et al. [3] propose a framework for participants of an organization to gain access to organizations' resources in a coalition environment with syntactically and schematically heterogeneous policies. Pan, Mitra and Liu [4] propose a Semantic Access Control Enabler middleware-based system that uses organizations' ontologies to achieve information interoperability by defining two sets of relations: one for interlinking roles between organizations and another for interlinking (grouping) objects under semantic equivalent concepts. Koshutanski and Maña [5] present a platform-driven access control model that takes advantage of semantics of partners' requirements to provide interoperable access control to coalition resources composed of heterogeneous requirements.

Our approach provides a complimentary solution to leverage cross-organizational authorization policy enforcement, for example, by guaranteeing assurance requirement that organizations' individual authorization policies are certified. A certification of an authorization policy will ensure that a declared policy is correctly enforced by the corresponding underlying enforcement mechanisms. Especially in cases where part of a coalition workflow is executed on a remote partner's platform. Our approach will compliment the coalition-level authorization with assurance that all participating partners will conform to authorization policy certification during coalition formation and operation.

B. *Policy-driven Coalition Regulation Assurance*

There are several approaches targeting coalition-level policy regulation of independently defined partners' policies. A coalition policy specification governs coalition-level interactions where each partner of the coalition has its own internal policy regulating its participation and service provisioning to the coalition.

Wasson and Humphrey [6] propose a model for defining a policy governing VO operations composed by several partners. It uses a VO-wide operational policy along with VO policy on resources and VO policy on users. Lin et al. [7] propose a Trust-based Access Control combining global and local trust relationships among VO's parties.

Djordjevic, Dimitrakos et al. [8] propose an architecture that supports grid-enabled dynamic VOs. They propose a dynamic security perimeter solution that defines a boundary of a set of agents, services and resources, which collaborate to form a business process. Their motivation is to capture the dynamic notion of VOs by means of perimeters, where each perimeter can dynamically shrink or expand its membership.

Ao and Minsky [9] propose a model and an enforcement mechanism for flexible regulation of distributed coalitions. Their work lays down some important elements of how to approach composition of individual partners' policies into scalable and computationally feasible coalition-level policy governance.

Our approach presents a complimentary solution to those approaches by providing security assurance for partners' services without the need to know the providers of all services in a composition (see discussion in Section VI.A).

C. *Certification-driven Service Security Assurance*

Service Oriented Computing (SOC) has facilitated a paradigm shift in software provisioning models: software gets consumed as a "service" providing enormous benefits. However lack of security assurance of third-party services is hampering their wider adoption in businesses, especially in dynamic collaborative environments.

Certification schemes such as Common Criteria are well established and quite successful in providing security assurance to consumers in a scalable manner. However, current certification schemes result in certificates that are represented in natural language, which do not cope well with the dynamic service environment. For service consumers, the possibility to compare the certified security features of a service with their security requirements is a relevant aspect in the service selection process. Several EU initiatives propose models and supporting methodologies of digital certificates addressing service security assurance, such as the ASSERT4SOA[1] and CUMULUS[2] EU projects. The former project focuses on SOC environments while the latter project focuses on cloud environments.

Particularly, a result of ASSERT4SOA project on a certificate model and language, called ASSERT [10], is closely related to our needs targeting coalition operation assurance in a SOC-based platform environment. The ASSERT language allows fine-grained expression of security properties, the target of certification, evaluation-specific evidences supporting the certified security property (such as model-based, test-based), service binding information (ensuring binding of the ASSERT certificate to the corresponding service). ASSERT certificates have XML-based structure and machine processable representation of security features of services.

Another relevant result of the ASSERT4SOA project regards the security assurance (certification) of service compositions and the concept of "virtual certificate" for service compositions [11] [12]. The cornerstone of the approach is the use of predefined *orchestration patterns*, which are *a priori* proven to support certain workflow properties given the individual services of the composition exhibits certain security properties. These patterns aim at providing additional level of automation to workflow certification activities; given the fact a workflow matches some of those patterns.

The actual certification process undertaken by a certification authority to certify coalition workflow properties is assumed to occur outside the proposed framework. As such, the means of design-time analysis of workflow security are not considered in the paper.

IV. HDC Security Assurance Conceptual Model

We define the following conceptual model of HDC security assurance, shown in Figure 1. We clustered the model in five major planes, as a stack view, to clearly position and separate the conceptual aspects and specifics of the proposed model.

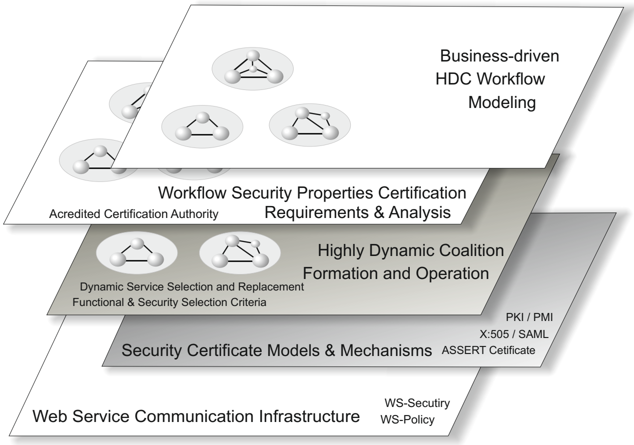
Business-driven
HDC Workflow
Modeling
Workflow Security Properties Certification
Requirements & Analysis
Acredited Certification Authority
Highly Dynamic Coalition
Formation and Operation
Dynamic Service Selection and Replacement
Functional & Security Selection Criteria
PKI / PMI
X:505 / SAML
ASSERT Cetificate
Security Certificate Models & Mechanisms
Web Service Communication Infrastructure
WS-Secutiry
WS-Policy

Figure 1: HDC Security Assurance Conceptual Model

Business-driven HDC Workflow Modeling: This plane defines business-driven workflow modeling of HDC. It deals with the task of defining (abstract) business models, including requirements for partners, along with their roles and services. Unlike static coalitions and VOs where business models can include references to specific partners' services used, in a HDC scenario the specific partners providing such services become known only when a coalition formation request is received. Thus, this layer defines abstract business workflows where exact service providers are not defined yet.

HDC Workflow Security Properties Certification: This plane defines non-functional security requirements for partners in HDC models. The need to ensure security on potential partners' services within HDC (abstract) workflow model calls for certified descriptions of partners' services for non-functional aspects such as security properties. This layer provides assurance by means of certification models and processes undertaken by accredited certification authorities. The outcome of a certification process is a digital certificate expressing the security properties of the HDC workflow conditioned by the security properties each involved service

[1] http://www.assert4soa.eu

[2] http://www.cumulus-project.eu

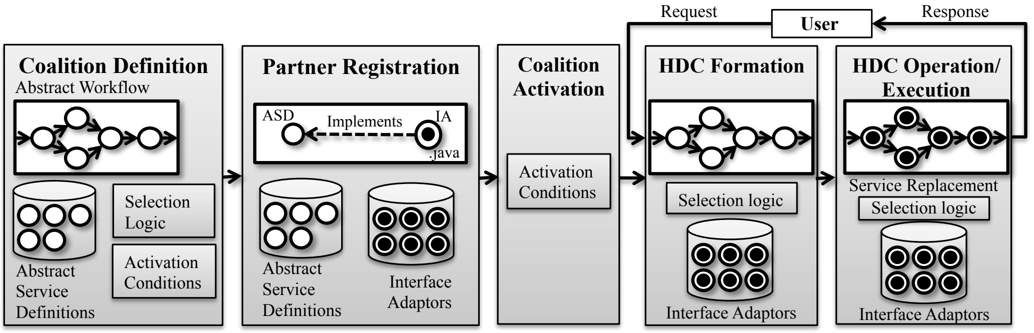

Figure 2: HDC Lifecycle

must provide. The security properties required for an abstract service definition must be ensured by the underlying layers.

HDC Formation and Operation: This plane defines all building blocks underlying HDC formation and operation aspects. The important characteristic of this plane is the automated formation of coalitions and fulfillment (operation) of HDC goals with provision of the desired services. The goal of this plane is to enable fully automated coalition formations and operations by supporting dynamic service selection, replacement and re-composition without sacrificing required trust and security assurance aspects.

Security Certificate Models & Mechanisms: This plane supports security certificate models and mechanisms necessary to practically realize the HDC workflow operational assurance model. It supports security certificate standards for identity and authorization management such as X.509 [13] and SAML [14], and supports digital certificates for expressing security aspects of services, such as the ASSERT language [10]. The identity and attribute certificates enable partners' authentication and authorization when accessing platform's facilities (e.g., partner registration and profile management), as well as bootstrapping any secure and trusted communications between the platform and the remote partners' services (such as WS-Security, SSL, etc.).

The support for service security certificates enable the platform to verify (ensure) if partners' services are certified and conform to the required security properties of the corresponding abstract service definitions. The important aspect here is that the supported service security certificate models enable machine processability of the certified security properties to allow automated conformance verification of partners' services. The last aspect will ensure conformance of partners' certified services to the required security properties during automated coalition formation and dynamic service replacement.

Web Services Communication Infrastructure: The bottom layer of the figure shows a targeted underlying computing and communication infrastructure, supporting Web service-oriented computational and communication standards.

A. Platform Role

The paper proposes a platform-driven environment equipped with appropriate security certificate models and technologies for the realization of workflow operational assurance. A platform-driven coalition operational model will allow for highly dynamic and automated coalition formations without sacrificing required trust and assurance aspects. It will enable a unified processing and enforcement of security-by-design certificated security properties for partners participating in HDCs, and will bootstrap coalition operation with high-level of security assurance. The goal is to provide scalable (for a large number of partners), efficient (for automated formations), and practical realization of the HDC workflow operational assurance model.

The proposed platform environment operates on planes 3 and 4, as shown in Figure 1. It offers several services dedicated to facilitate the HDC life cycle, such as defining, creating and managing HDC models, and registering partners (service providers), as we will see in the next section.

V. HDC LIFECYCLE

The HDC lifecycle is divided into the following five phases: coalition definition, partner registration, coalition activation, coalition formation and coalition operation. These phases are shown in Figure 2. To achieve the necessary dynamism the coalition activation, formation and operation phases are defined to be completely automated.

HDC workflow design activities particular to plane 1, as shown in Figure 1, take place prior to the platform operation. For example, one can adopt any BPEL-based workflow design environment, such as Oracle BPEL Process Manager[3], that supports design and definition of BPEL processes, and conversion from BPEL-based workflow specification to an executable code of the workflow (e.g., Java-based). Alternatively, one can define a service-based coalition workflow without going through any BPEL-like design phase, thus providing the workflow directly as executable code.

Coalition Definition. The coalition creator will use the platform services in order to register the *executable code*[4] of the abstract workflow of the HDC model (as a service) and the corresponding set of *abstract service definitions* (ASDs) that constitute the abstract workflow. The concept of ASD is central to the platform functionality as it allows the HDC creator to define functional and non-functional requirements for each service, as part of its ASD, which have to be enforced (ensured) during formation and operation phases. The coalition creator also defines *coalition selection logic* of how suppliers are selected to be part of the coalition as most likely there will be multiple providers per service (i.e., for each ASD). The purpose is to define and automate the selection process of partners that best fit the coalition goals.

Another important part of coalition definition phase is the definition of *coalition activation conditions*. Those conditions are defined to indicate when an HDC abstract workflow can

[3] http://www.oracle.com/technetwork/middleware/bpel

[4] Although an abstract workflow cannot be directly executed, still it has a corresponding code that is to be executed after selection of partners takes place.

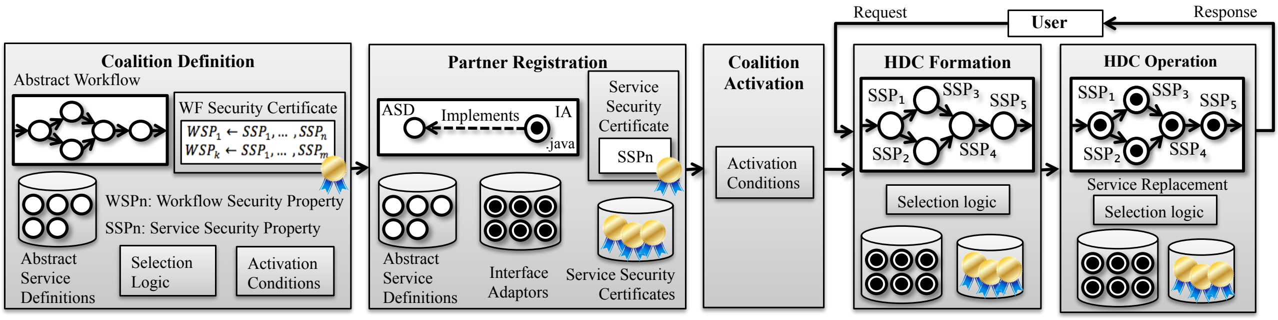

Figure 3: Security Assurance of Certified HDC Models through HDC Lifecycle

be made active and available as a service to end-users. For example, a default activation condition is that at least one service provider registered per ASD of the HDC workflow, or at least N number of providers per given ASDs must be registered in order to guarantee certain availability for some functional aspects of the workflow. One can also use functional and non-functional service aspects to enforce more complex activation conditions.

The goal of the HDC lifecycle to fully automate the coalition formation phase by ensuring that all activated HDC workflows, which satisfy the coalition activation conditions, will provide a necessary level of guarantee that coalition formation phase will succeed to instantiate a given abstract workflow.

Partner Registration. Service Providers (SPs) will use dedicated platform services in order to register themselves on the platform to provide their services and thus extend/enrich their potential customers. A SP can explore an abstract service definition catalogue, and for any ASD he selects to provide an actual service, the SP uploads an *interface adaptor* (IA) that implements the ASD by using the SP's external services. The interface adaptor plays a central role to enable the technical realization of the HDC platform approach. The main role of IA is to provide a "bridge" between the ASD defined service interface and the corresponding partner's *remote* service interfaces that implement an actual ASD functionality. The IA is in charge of making a remote call to the partner's services and adapting (if necessary) messages between the interfaces.

Coalition Activation. An automated phase that triggers coalition activation when coalition activation conditions are satisfied. The coalition activation phase is in charge of activating and publishing HDC models on the platform as services to end-users so that potential clients are able to use the platform in order to request HDC services.

Coalition Formation and Operation. The last two phases are bound to perform upon user request to a coalition service. The important characteristic is the automated coalition formation process that performs dynamic partners selection that most fit the coalition goals. Based on the defined selection logic, the technical outcome of the selection process is the set of interface adaptors per ASD of the coalition workflow. The coalition operation (execution) phase is triggered automatically based on the results of the selection process of the coalition formation phase.

During coalition operation, if for a selected SP's IA, already part of an activated coalition, the corresponding partner's (remote) service is unavailable for some reasons, a dynamic service replacement process is triggered based on the selection logic procedure in order to re-select (if available) another SP's IA for the corresponding ASD.

A. *HDC Reusability*

The HDC lifecycle model allows coalition creators to reuse existing ASDs in order to utilize service providers who are already taking part of the platform in their new HDC models. A catalogue of public ASDs with specific service functional and non-functional requirements is available to coalition creators. A coalition creator upon defining an ASD decides whether the ASD can be public – available for use within other HDC models of the platform, or private – restricted for use by predefined set of service providers in predefined HDC models.

A coalition owner of an already active HDC can provide an interface adaptor of the HDC service for an ASD of a different HDC model, thus making the active HDC coalition service as a registered partner's service for another HDC model of interest.

VI. Security Assurance of Certified HDC Models

Based on the design specification of the HDC workflow (e.g., BPEL-based) and its corresponding executable code, a coalition owner can request an accredited authority to undertake a certification process on the desired security aspects of the workflow and issue a certificate bound to the executable code of the abstract workflow[5].

Once the HDC workflow has been certified, during coalition definition phase, the coalition owner defines the certified security properties of the workflow by supplying the workflow security certificate that will be the basis to actually define the required security properties for each ASDs of the workflow. The platform will *verify* the workflow security certificate, for example, if issued by accredited authority and if the registered workflow executable code is the one the certificate is bound to. The workflow security properties are conditioned by the required assurance for the defined security properties of individual abstract service definitions of the workflow. In other words, a workflow security property holds only if the required security properties of the ASDs are preserved by selected partners' services during the coalition formation phase.

Figure 3 shows the enriched HDC lifecycle addressing security assurance of certified HDC models. We have enriched

[5] We note that an authority can also issue a certificate bound to a BPEL specification of the workflow (but not to code). In such case the platform has to provide the corresponding functionality of transforming from BPEL to executable code, which requires an additional level of assurance for correctness of such transformation.

the partner registration phase by requiring partners interested in providing services to a particular ASD of a given HDC workflow to provide not only the corresponding IA implementing the ASD but also a set of *service security certificates* stating the required security properties of the given ASD. An important aspect here is that service providers provide security assurance for their services by means of digital security certificates. The service security certificates are *verified* by the platform to ensure the required security properties for an ASD are met by certified security properties of the partner's service. A *successful* partner's service registration process is achieved when the required security properties are met by the certified service.

The ASSERT certificate model of ASSERT4SOA project can be used as a possible realization of security assurance of partners' services. The ASSERT model and language provide the necessary ground to enable automated machine processing (inference and matching) on service certified security properties and related evidences supporting the properties. The adoption of the ASSERT model will enable the realization of the identified security assurance aspects during the partner registration phase.

Furthermore, the enriched partner registration phase provides security assurance to the coalition formation phase by ensuring that for all activated HDC models coalition formation will succeed to instantiate the abstract workflows by selecting partners already verified to satisfy the requires security properties of the individual workflow services. Thus, at coalition formation and operation, the provided security certificates do not need to be verified again if meet the security requirements but will need to undergo only basic verification if the certificates are still valid and not revoked.

In case of multiple partners' services registered for an ASD, it is necessary to define a mechanism to select not only the partners that satisfy the functional requirements but among those to select the ones with *higher assurance* on required security properties. This last aspect is very relevant for both coalition formation and operation phases.

The ASSERT4SOA service discovery engine [15] can be well adopted to address the issue of discovering those partners' services (among the registered ones) having highest assurance with respect to the required security properties of a given ASD. The main benefit in adopting the ASSERT4SOA approach is that different *dimensions of security assurance* can be achieved depending on exact preferences one defines for ordering providers' services, such as based on types and strength of security mechanisms supporting the certified security properties, preferences on evaluation type evidences supporting the certified security properties (e.g., formal model-based over test-based), and types of service models.

As discussed in Section III, security certification of service compositions [11][12] adopts the use of predefined orchestration patterns, a priori proven to support certain workflow properties given the individual services of the composition exhibits certain security properties. These approaches can give an interesting ground to enable *virtual certification* of HDC workflows without requesting a certification process to a given authority. In our platform settings, these approaches can be very valuable for those HDC workflows that cannot afford going through authority certification process but which match some of the predefined orchestration patterns with (manually) proven security properties. In such a case, the platform can still address security assurance for those workflows by requiring partners registering to services of those workflows conform to required security properties stated in the orchestration patterns. In such case, the assurance comes from the authority that certified an orchestration pattern.

A. Platform Assurance Model

There are several roles of certification authorities considered in the platform assurance model. A certification authority role certifying workflow security (service composition). A certification authority role certifying security features of partners' services. A certification authority role certifying interface adaptors supplied to the platform.

If we look closely in the assurance chain build, from the one side, there is an assurance coming from the certified workflow security, and from the other side, there is an assurance coming from the certified partners' services. However, the concept of IA stays in between the two sides of the assurance model, playing the role of adapting the interface messages between the defined ASD and actual partner's service interfaces.

Since the platform will be responsible for hosting and executing the provided IAs (but not the remote partners' services), consequently, we defined the role of a *platform authority* to examine and approve (certify) whether partners' supplied IAs *preserve* the security properties the corresponding partners' service are certified for. This process of IA approval takes part during partner registration phase and is a condition for a successful outcome of partners' services registration to the platform.

Since examining IAs whether they preserve given security properties will require a dedicated expertise to assure the properties are preserved, we define the role of the platform authority to adequately *complete* the platform assurance model. Another element underpinning the platform assurance model is the fact that in most cases the IAs will exhibit simple logic of message alignment between interfaces so that the IA approval process (or IA certification) is expected to be light and efficient in terms of effort and time.

The platform model provides the following assurance:

- *Service providers assurance*: Service providers wishing to provide services to a HDC certified model will have assurance for the overall workflow security aspects and for individual services' security aspects. The platform model provides assurance to service providers that the security of the certified workflow will be preserved (guaranteed) as certified, even without knowing the exact partners that will be selected during the coalition formation and coalition operation phases.
  Motivating the need to have providers' assurance is the case where a service provider has sensitive market analysis information that wishes to provide in HDC models. The partner will be willing to register for those certified HDC models assuring confidentiality of data exchange on the overall workflow. In contrast, a HDC workflow may be certified to guarantee confidentiality of data in transit among services in a composition but not in storage of such data. In the last case, confidentiality may not be sufficient to assure confidential treatment of the

provided market analysis data when storage is not protected, as there might be potential leak of that information to undesired third parties.

- *Coalition users assurance*: Coalition users will have assurance that whenever requesting coalition services the most adequate coalition formation (partner selection) will be selected preserving the certified workflow properties.

The platform model has several dimensions of workflow operational assurance:

- Assurance coming from the trust in authority certifying the workflow.
- Assurance coming from the trust in platform correctness in selection of partners. This aspect can be subject of external authority certification attesting the correctness of the platform selection mechanism. In that case, assurance can be further leveraged by the trust in the authority certified the coalition platform.
- Assurance coming from the trust in authorities certified partners' services.
- Assurance coming from the trust in the platform authority in certifying (approving) partners IAs. The assurance in this aspect can be further leveraged by having the platform authority be accredited (certified by a third-party recognized authority) as being capable of approving whether IAs preserve security properties.

VII. HDC Security Assurance of Scenario

In this section we will illustrate the process of creating and using a HDC to achieve the desired security assurance of the scenario in Section II. The HDC model offers a service to end-users with input a list of Quote Requests, where each Quote Request consists of: (i) *Company* - The company whose shares a user wants to buy; (ii) *Quantity Threshold* - The maximum shares a user wants to buy for that particular company; and (iii) *Price Threshold* - The maximum amount a user wants to spend on that company's stock.

The BROKO HDC service offers the following methods to clients: *Get User Preferences* - handles an input of a Quote request; and *Get User Confirmation* - shows an investment summary to the final user and make him able to confirm or reject the operation. When confirmed the investment is done. The HDC workflow process must analyze the user's requests and match them against stocks based on their current and predicted value along with insurance and tax information, and finally buy the stocks with the user approval.

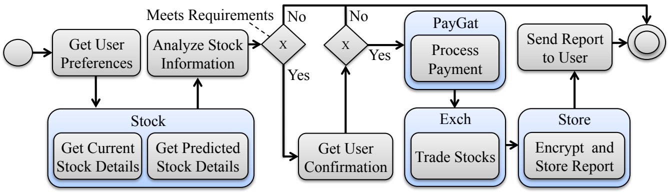

Figure 4: Stock Brokerage Workflow

Figure 4 shows the identified HDC workflow of the scenario. Each grey box represents a method that will use and process the user request data. The blue boxes are the abstract service definitions and the methods that are inside them will be *externally executed* on the supplier's remote servers, while the other methods will be executed *locally* on the platform.

The methods of the other services are the following: **PayGat:** `Process Payment` – takes as input of Sender, Recipient and the transaction amount. **Ecxh:** `Trade Stocks` – takes as input of Buyer information and the stock information along with the quantity. **Store:** `Encrypt and Store Report` – takes as input of a report and the file meta information.

Once the HDC abstract workflow is designed BROCKO will request a certification process to address security assurance of the newly designed workflow. For doing so, BROCKO consuls with an accredited certification authority on the needed security properties that are to be guaranteed by the workflow. The outcome of the certification process on the workflow is summarized in the table below. For the sake of simplicity, we have limited the certification to one workflow security property – confidentiality of user and stock data. That is, all user and stock data must be transmitted and stored confidentially protecting both information related to the investment request and personal information of the user.

Workflow Security Property		
Abstract Security Property	***Property Context***	***Assets***
Confidentiality	In transit	User & Stock Data
Confidentiality	In storage	User & Stock Data

Service Security Assurance Requirements			
ASD	***Abstract Security Property***	***Property Context***	***Assets***
Stock	Confidentiality	In transit	Current Stock Data
			Predicted Stock Data
PayGat	Confidentiality	In transit	Payment Order Data
			Payment Confirmation Data
Exch	Confidentiality	In transit	Stock Purchase Order
			Stock Purchase Confirmation
Store	Confidentiality	In transit	Data Storage Request
			Data Storage Confirmation
	Confidentiality	In storage	Report and Report Meta Data

To hold the workflow property, the required individual service security properties are defined accordingly. Once the HDC workflow is designed and certified accordingly, the coalition owner can now use the platform services to define the coalition and its corresponding data.

Coalition Definition. The coalition creator uploads the executable code of the abstract workflow and the security certificate of the workflow. Next, the platform verifies the certificate to ensure the certificate is issued by an accredited authority (trusted by the platform) and that the certificate corresponds to the uploaded workflow. Once the HDC workflow is defined, the coalition owner defines the set of Abstract Service Definitions (ASDs) corresponding to the workflow. We will only show a summary of ASD metadata corresponding to the Stock Broker service shown in the table below. The ASDs for the rest of the services can be analogously done.

Stock Broker ASD	
Name	Stock
Methods	GetCurrentStockDetails: takes as input a company code and returns the current stock value.
	GetPredictedStockDetails: takes as input a company code and returns the predicted stock value.
Functional	Required Markets: UK, Spain or France.

Requirements			
Non-functional Requirements: Performance	Timeout: 3 sec		
Non-functional Requirements: Security	Confidentiality	In transit	Current Stock Data
			Predicted Stock Data

Partner Registration. Let us assume a partner called Andalucía Stock Broker S.L. offers stock-broker services to clients restricted in the Spain market. The Andalucía Stock Broker S.L., among its services, offers two particular services, called StockInfo and StockPrediction. Both services are certified providing security assurance to its consumers for security property *confidentiality* in context *transit* on assets *stock data request* and *stock data response*. The certificates represented using the ASSERT language for StockInfo service[6] and for StockPrediction service[7]. Given that, the Andalucía Stock Broker S.L. can register as a service provider to the corresponding ASD, named above as Stock, by uploading an IA and the two ASSERTs. Particularly, the uploaded IA[8] implements the ASD interface such that for the operation GetCurrentStockDetails it calls a getStockInfo operation of the StockInfo service, and for the operation GetPredictedStockDetails the IA calls a getStockPrediction operation of the StockPrediction service.

Once the IA and the two ASSERTs are provided to the platform, the platform authority will have to examine if the IA code and the two certificates meet the required security property of the ASD, and approve registration of Andalucía Stock Broker S.L. as a provider for the ASD called Stock.

Coalition Activation. Let us use a simple activation rule: at least *three* service providers registered to the Stock ASD and at least *one* provider for the other services in the coalition.

User Request: *Company*: Santander Group; *Quantity Threshold*: 100 shares; *Price Threshold*: 6 Euros per share.

Coalition Formation and Operation. The BROCKO workflow is instantiated and executed with an optimal set of partners for the given user request.

VIII. Conclusions and Future Work

Given the pervasive usage of dynamic collaborative environments to address cost-effective and competitive business aggregation, the security assurance of a coalition workflow operation becomes more and more important since partners participating in a coalition will likely have heterogeneous security models for service provisioning.

The proposed platform approach aims at assuring the certified coalition workflow security properties during coalition formation and operation phases, which are of primary concern for both the users of coalition services and providers of those services. An important aspect of the proposed workflow assurance platform is the adoption of a *certificate model*, in our case ASSERT, that captures service security aspects and enables automated machine inference of certified service security properties to ensure partners' services conform to required security properties, and to leverage automated selection of partners with higher security assurance.

An important criterion for the adoption of the certificate model is that the underlying language artifacts of the certificate model should allow use of ontology vocabularies defined by different certification authorities for their respective schemes based on the certification/evaluation processes and the types of products certified.

Given that different certification authorities certifying workflow security properties and those certifying partners' services security properties may use different vocabularies to express security assertions in the certificate model, an important direction of future work is to define a *semantic abstraction layer* between certified workflow security properties and certified partners' service security properties to enable unified enforcement of security conformance of the coalition workflow assurance model.

IX. Acknowledgment

This work was partly supported by the EU-funded project ASSERT4SOA (grant no. 257361) under the EU FP7 program.

References

[1] H. Koshutanski and A. Maña: Highly Dynamic Coalitions - drive forward eBusiness. eStrategies magazine, British Publishers. February 2009. (http://www.projects.eu.com)

[2] Gartner, "Forecast overview: Public cloud services," report G00234817, 2012.

[3] Warner, J., Atluri, V., Mukkamala, R., Vaidya, J.: Using semantics for automatic enforcement of access control policies among dynamic coalitions. In: Proc. of the 12th ACM Symposium on Access Control Models and Technologies, (2007) pp. 235–244.

[4] Pan, C.C., Mitra, P., Liu, P.: Semantic access control for information interoperation. In: Proc. of the 11th ACM Symposium on Access Control Models and Technologies, (2006) pp. 237–246.

[5] Koshutanski, H., Maña, A.: Interoperable semantic access control for highly dynamic coalitions. Security and Communication Networks, Vol. 3, No. 6., Nov/Dec 2010, pp. 565--594. Wiley.

[6] Wasson, G., Humphrey, M.: Toward explicit policy management for virtual organizations. In: Proc. of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks, (2003) pp. 173–182.

[7] Lin, A., Vullings, E., Dalziel, J.: A trust-based access control model for virtual organizations. In: Proc. of the 5th International Conference on Grid and Cooperative Computing Workshops, 2006, pp. 557–564.

[8] Djordjevic, I., Dimitrakos, T., Romano, N., Randal, D.M., Ritrovato, P.: Dynamic security perimeters for inter-enterprise service integration. Future Generation Computer Systems 23(4) (2007) 633–657.

[9] Ao, X., Minsky, N. H.: Flexible Regulation of Distributed Coalitions. In: Proc. of the 8th European Symposium on Research in Computer Security. LNCS, Springer (2003) pp. 39–60.

[10] H. Koshutanski, A. Maña, R. Harjani, M. Montenegro, et al., "D1.2 ASSERT language v2," ASSERT4SOA Project, Tech. Rep., 2012, available at http://www.assert4soa.eu/deliverable/D1.2.pdf.

[11] M. Anisetti, C. A. Ardagna, E. Damiani, F. Saonara: A Test-based Security Certification Scheme for Web Services, ACM Transactions on the Web, 2013 (to appear).

[12] Pino L., Spanoudakis G.: "Constructing Secure Service Compositions with Patterns", In 8th IEEE World Congress on Services, June 2012.

[13] X.509, "The directory: Public-key and attribute certificate frameworks," 2005, ITU-T Recommendation X.509:2005 j ISO/IEC 9594-8:2005.

[14] SAML, "SAML specification," 2012. [Online]. Available: http://saml.xml.org/saml-specifications

[15] K. Mahbub, L. Pino, G. Spanoudakis, H. Foster, A. Maña, and G. Pujol, "D2.3 ASSERTs aware service based systems adaptation," ASSERT4SOA Project, Tech. Rep., 2012, available at http://assert4soa.eu/deliverable/D2.1.pdf

[6] ASSERT StockInfo Service available at http://proteus.lcc.uma.es/documentos/documentos/documento-94.xml

[7] ASSERT StockPrediction Service available at http://proteus.lcc.uma.es/documentos/documentos/documento-96.xml

[8] Interface Adaptor Andalucía Stock Broker S.L. at http://proteus.lcc.uma.es/documentos/documentos/documento-98.java