Security Infrastructure for On-demand Provisioned Cloud Infrastructure Services

Yuri Demchenko, Canh Ngo, Cees de Laat
System and Network Engineering Group
University of Amsterdam
Amsterdam, The Netherlands
e-mail: {y.demchenko, c.t.ngo, delaat}@uva.nl

Tomasz Wiktor Wlodarczyk, Chunming Rong
Department of Computer Science and Electrical Engineering, University of Stavanger, Norway
e-mail: {tomasz.w.wlodarczyk, chunming.rong}@uis.no

Wolfgang Ziegler
Department of Bioinformatics
Fraunhofer Institute SCAI
Sankt Augustin, Germany
e-mail: wolfgang.ziegler@scai.fraunhofer.de

Abstract—**Providing consistent security services in on-demand provisioned Cloud infrastructure services is of primary importance due to multi-tenant and potentially multi-provider nature of Clouds Infrastructure as a Service (IaaS) environment. Cloud security infrastructure should address two aspects of the IaaS operation and dynamic security services provisioning: (1) provide security infrastructure for secure Cloud IaaS operation; (2) provisioning dynamic security services, including creation and management of the dynamic security associations, as a part of the provisioned composite services or virtual infrastructures. The first task is a traditional task in security engineering, while dynamic provisioning of managed security services in virtualised environment remains a problem and requires additional research. In this paper we discuss both aspects of the Cloud Security and provide suggestions about required security mechanisms for secure data management in dynamically provisioned Cloud infrastructures. The paper refers to the architectural framework for on-demand infrastructure services provisioning, being developed by authors, that provides a basis for defining the proposed Cloud Security Infrastructure. The proposed SLA management solution is based on the WS-Agreement and allows dynamic SLA management during the whole provisioned services lifecycle. The paper discusses conceptual issues, basic requirements and practical suggestions for dynamically provisioned access control infrastructure (DACI). The paper proposes the security mechanisms that are required for consistent DACI operation, in particular security tokens used for access control, policy enforcement and authorisation session context exchange between provisioned infrastructure services and Cloud provider services. The suggested implementation is based on the GAAA Toolkit Java library developed by authors that is extended with the proposed Common Security Services Interface (CSSI) and additional mechanisms for binding sessions and security context between provisioned services and virtualised platform.**

Keywords-Cloud Security infrastructure,Cloud Infrastructure as a Service (IaaS), On-Demand Infrastructure Services Provisioning, Dynamic Access Control Infrastructure, Security Context Management.

I. INTRODUCTION

Cloud computing technologies [1, 2] are emerging as infrastructure services for provisioning computing and storage resources on-demand in a simple and uniform way. However there is no well-defined architectural model for the Cloud Infrastructure a Service (IaaS) provisioning model despite its wide use among big Cloud providers such as Amazon, RackSpace, Google, and others. Recent research based on the first wave of Cloud Computing implementation have revealed a number of security issues both in actual services organisation and operational and business models [3, 4, 5]. Current Clouds security model is based on the assumption that the user/customer should trust the provider. This is governed by the general Service Level Agreement (SLA) that defines mutual provider and user expectations and obligations for the whole provisioned services but doesn't allow dynamic Quality of Services (QoS) management in potentially *changing* resources availability due to changing resources demand and utilisation.in typically multi-user Cloud environment.

Although Cloud providers are investing significant resources into making their own infrastructure secure and complying existing security management standards (e.g. Amazon Cloud recently achieved PCI compliance certification [6] and announced providing special services for governmental organisations [7], Microsoft Azure claims ISO27001 compliance [8]), still the overall security of the Cloud based infrastructures and services will depend on the two other factors: security services implementation in user applications and binding between virtualised services and Cloud based virtualisation platform, that should also ensure protection against malicious users and risks related to possible Denial of Service (DoS) attacks.

Practical Cloud usage within one provider infrastructure creates illusion of unlimited availability, "elasticity" and "perfect" security (as claimed by the providers themselves), but in practice this is related only to limited range of services and with limited manageability. Currently implemented and offered security services are based on VPN and provide only simple access control services based on users access over SSH channel. Recent improvements in GooglApps allow SAML based Single Sign-On (SSO) [9] to connect/integrate Cloud based services and customer legacy access control infrastructure. More advanced security services and fine grained access control cannot be achieved without deeper integration with the Cloud virtualisation platform and incumbent security services, what in its own turn can be achieved with open and well defined Cloud IaaS platform architecture to allow transparent interoperability and integration of heterogeneous multi-provider Cloud infrastructure services.

Current development of the Cloud technologies demonstrate movement to developing inter-Cloud models, architectures and integration tools that could allow integrating Cloud based infrastructure services into existing enterprise and campus infrastructures, on one hand, and provide common/interoperable environment for moving existing infrastructures and infrastructure services to virtualised Cloud environment. More complex and community oriented use of Cloud infrastructure services will require developing new service provisioning and security models that could allow creating complex project and group oriented infrastructures provisioned on-demand and across multiple providers.

The paper presents the ongoing research aimed at developing a framework that will address known problems in provisioning consistent security services for dynamically provisioned and reconfigurable infrastructure services that may include both computing resources (computers and storage) and transport network.

The papers refers to the architectural framework for provisioning Cloud Infrastructure Services On-Demand [10, 11] being developed by authors in a number of currently running projects such as GEANT3 [12] and GEYSERS [13] that provides a basis for defining the proposed security infrastructure for Cloud IaaS. The presented in this paper research targets developing a consistent security services infrastructure for dynamically configurable Cloud infrastructure services provisioned on demand.

The paper is organized as follows. Section II discusses the generalised architecture and operational model for on-demand infrastructure services provisioning that is used for defining general requirements to dynamically provisioned security services. Section III discusses the security paradigm shift in Cloud Computing and summarises the basic security requirements to dynamically provisioned security services and secure data management in Cloud. Section IV provides short reference to the Security Services Lifecycle Management (SSLM) [14] model proposed in another authors' work as an important component of the whole IaaS security infrastructure. Sections V discusses the Dynamic Access Control Infrastructure (DACI) operation during the services provisioning stages and provides implementation suggestions for some of the proposed security mechanisms. Section VI discusses SLA management issues and proposes an approach to maintain important SLA guarantees during the provisioned services operations. Section VII discusses implementation suggestions of proposed DACI components such as security session management mechanisms and security services interfaces.

II. ON-DEMAND INFRASTRUCTURE SERVICES PROVISIONING

Figure 1 below illustrates the abstraction of the typical project or group oriented Virtual Infrastructure (VI) provisioning process that includes both computing resources and supporting network that commonly referred as infrastructure services. The VI is provisioned for two collaborative user groups in different locations that in order to fulfill their task (e.g. cooperative image processing and analysis) require a number of resources and services to process raw data on distributed Grid or Cloud data centers, analyse intermediate data on specialist applications and finally deliver the result data to the users/scientists. The discussed use case contains all basic components of the typical e-Science research process: data production with scientific instrument (labeled as VIR4 node), initial data mining and filtering (VIR3, VIR5), analysis with special scientific applications (VIR1, VIR6), and finally presentation and visualisation (VIR1, VIR6) to the users.

The main actors involved into this process are Physical Infrastructure Provider (PIP), Virtual Infrastructure Provider (VIP), Virtual Infrastructure Operator (VIO). The required supporting infrastructure services are depictured on the left side of the picture and include functional components and services used to support normal operation of all mentioned actors. The Virtual Infrastructure Composition and Management (VICM) layer includes the Logical Abstraction Layer and the VI/VR Adaptation Layer facing correspondingly lower PIP and upper Application layer. These layers represent interfaces used by VIO and user applications to access VIR and support necessary logical transformation of the resources during composition and operation stages.

Figure 1 also shows trust domains related to VIO, VIP and PIP that are defined by the corresponding trust anchors (TA) denoted as TA1, TA2, TA3. The user (or requestor) trust domain is denoted as TA0 to indicate that the dynamically provisioned security infrastructure is bound to the requestor's security domain. The Dynamic Security Association (DSA) is created as a part of the provisioning VI. It actually supports the VI security domain and is used to enable consistent operation of the VI security infrastructure.

The infrastructure provisioning process, also referred to as the Service Delivery Framework (SDF) defined in [11], implements and extends the related TeleManagement Forum SDF definition [15]. It includes the following main stages: (1) infrastructure creation request sent to VIO or VIP that typically includes SLA that specifies required services and may also include trust anchor to bind the user and the VIO trust domains; (2) infrastructure planning and advance reservation; (3) infrastructure deployment including services synchronization and initiation; (4) operation stage, and (5) infrastructure decommissioning. SDF combines in one provisioning workflow all processes that are run by different supporting systems and executed by different actors. The SDF operation is supported by the Service Lifecycle Metadata Service (MD-SL) that maintains VI and component services identifies, stages, versions and binds them to the SLA and provisioning sessions IDs.

Physical Resources (PR), including IT resources and network, are provided by Physical Infrastructure Providers (PIP). In order to be included into VI composition and provisioning by the VIP they need to be abstracted to the Logical Resource (LR) that will undergo a number of abstract transformations, including possibly also interactive negotiation with the PIP. The composed VI need to be deployed to the PIP which will create virtualised physical resources (VPR) that may be a part or a pool of the resources provided by PIP. The deployment process includes distribution of common VI context, configuration of VPR at PIP, advance reservation and scheduling, and virtualised infrastructure services synchronization and initiation, to make them available to Application layer consumers.

The proposed architecture provides a basis and motivates development of the generalised framework for provisioning dynamic security infrastructure that includes the Dynamic Access Control Infrastructure (DACI), Security Services Lifecycle Management model (SSLM), Common Security Services Interface (CSSI), and related security services and mechanisms to ensure the consistency of the dynamically provisioned security services operation. The required security infrastructure should provide a common framework for operating security services at VIP and VIO layer and be integrated with PIP's legacy security services.

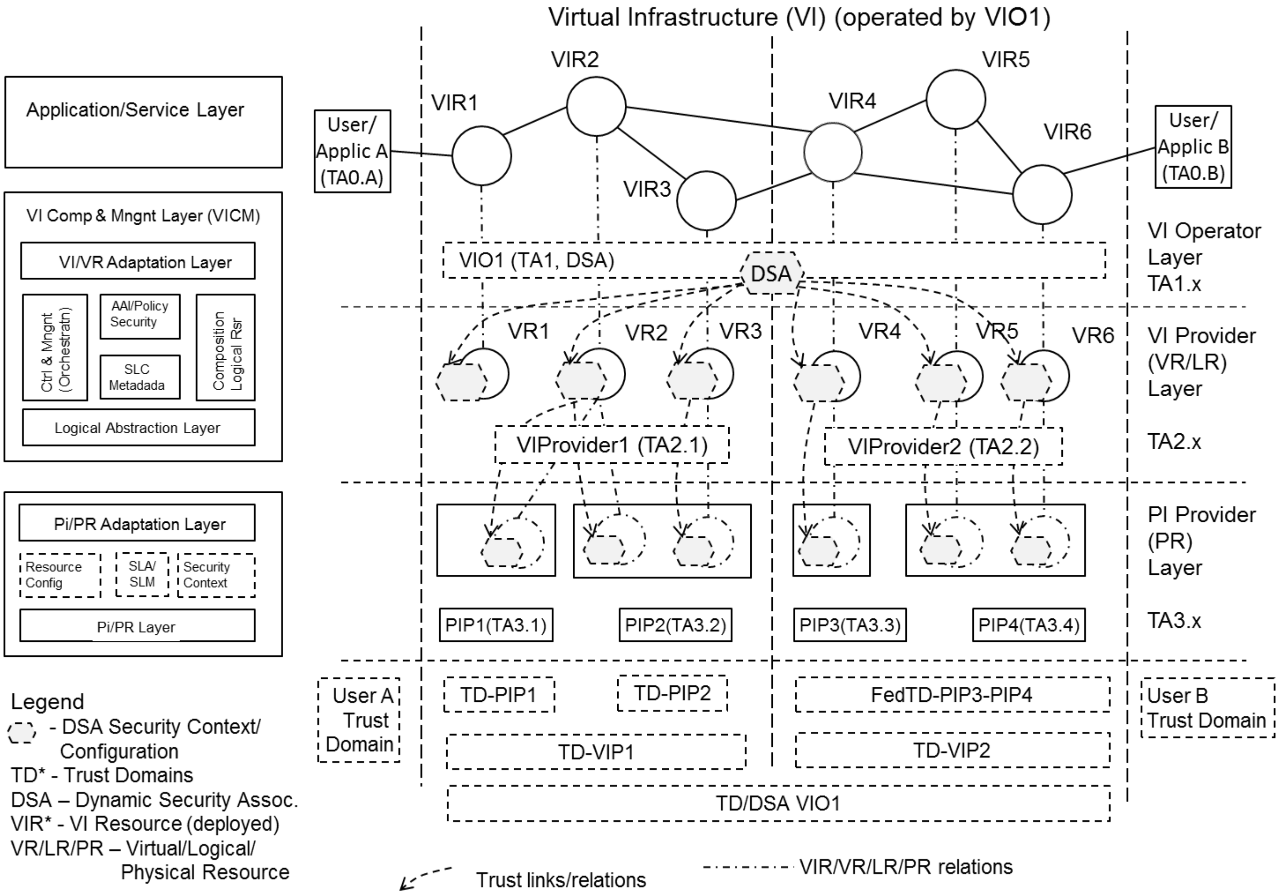

Figure 1. Main Actors, Functional Layers and Trust Relations in On-Demand Infrastructure Services Provisioning.

It is important to mention that discussed here physical and virtual resources are in fact complex software enabled systems with their own operational systems and security services. The VI provisioning process should support their smooth integration into the common federated VI security infrastructure what will allow defining and using common access control models and policies. Access decision made at the VI/VIO level should be trusted and validated at the PR/PIP level, however final authorisation decision should be a subject to the local (to the protected resource or services) policy decision. This can be achieved by creating the DSA during the provisioning process as illustrated by Figure 1.

The proposed architecture is based on the Service Oriented Architecture (SOA) [16] and uses the same basic operational principles, which provides a direct mapping to the possible VICM implementation platforms such as Enterprise Services Bus (ESB) or OSGi framework [17, 18].

III. DYNAMICALLY PROVISIONED SECURITY SERVICES

A. *Paradigms Change and General Challanges*

On-demand provisioning of virtualised Cloud infrastructure services drives paradigm change in security design and operation. Considering evolutional relations between Grids and Clouds, it is interesting to compare their security models. This is also important from the point of view that future e-Science infrastructures will integrate both Grid based core e-Science infrastructure and Cloud based infrastructures provisioned on-demand. Deploying native/original Grid services on Clouds [19]. Grid security architecture is primarily based on the Virtual Organisations (VO) that are created by the cooperating organisations that share resources (which however remain in their their ownership) based on mutual agreement between VO members and common VO security policy. In Grids, VO actually acts as a federation of the users and resources that enables federated access control based on the federated security and trust model [20, 21].

The following problems/challenges arise from the Cloud IaaS environment analysis for security services/infrastructure design:

- Data protection both stored and "on-wire" that include beside necessary confidentiality, integrity, access control services, also data lifecycle management and synchronization.
- Access control infrastructure virtualisation and dynamic provisioning, including dynamic/automated policy composition or generation.
- Security services lifecycle management, in particular related services metadata and properties, binding to main services.
- Security sessions and related security context management during the whole security services lifecycle, including binding security context to the provisioning session and virtualisation platform.
- Dynamic security associations (DSA) and trust/key management, including virtual infrastructure trust anchors bootstrapping during deployment stage, what should provide fully verifiable chain of trust from the user client/platform to the service/data runtime environment.
- SLA management, including initial SLA negotiation and further SLA enforcement at the planning and operation stages.

Initial suggestions to address those problems require the consistent provisioning and applications security sessions management, in particular:

- Session synchronization mechanisms that should protect the integrity of the remote run-time environment.
- Secure session fail-over that should rely on the session synchronization mechanism when restoring the session.
- Special session for data transfer that should also support data partitioning and run-time activation and synchronization.
- Standardized interfaces that will answer some of user concerns on cloud security.

Wider Clouds adoption by industry and their integration with existing legacy infrastructure services will require implementing manageable security services and mechanisms for the remote control of the Cloud operational environment integrity by users.

B. *Data Security*

In the Clouds data are sent to and processed in the environment that is not under the user or data owner control and potentially can be compromised either by Clouds insiders or by other users sharing the same Cloud platform or resources. Data/information must be secured during all processing stages – upload, process, store, stream/visualize. Policies and security requirements must be bound to the data and there should be corresponding security mechanisms in place to enforce these policies.

The security solutions for data handling in Clouds should cover the following compatibility scenarios in order to eliminate user concerns on cloud security that arise from perceived loss of control over data while using Cloud services:

Separation: to enable separation between processing and storage services (with assumption that they will not collude).

Availability: to ensure data availability to user if provisioned service goes off line.

Migration: to provide independence of storage service provider.

Tunneling: to provide guarantee against colluding in separation scenario.

Cryptography: to guarantee confidentiality and integrity in tunneling service.

The security solutions and supporting infrastructure should address the following problems, mostly related to the data integrity and data processing security:

- Secure data transfer that possibly should be enforced with the data activation mechanism
- Protection of data stored on the Cloud platform
- Restore from the process failure that entails problems related to secure application session and data restoration.

Existing approaches to data protection are based on the assumption that the user trusts the cloud provider. However in many application areas the data owners would like to have control over data access and use in untrusted environment. The protocol proposed by Zhao et al. [22] can imperatively impose the access control policies of data owners preventing the cloud storage providers from unauthorized access and making illegal authorization to access the data. The protocol is based on the progressive curve encryption scheme. It allows a piece of data to be encrypted multiple times using different keys in such a way that the final ciphertext can be decrypted in a single run with a single key.

Several interfaces are defined in [23] to provide consistent data management security. They should be implemented by respective services in the SOA-based infrastructure to ensure interoperability in data security services management:

- Data Access Interface (DAI). DAI should be a standard-based interface implemented by services providing storage functionality. It can be then used by services providing processing functionality to access data. Often one actual service might both functionalities; however, such formal division is suggested in order to ensure flexibility.

- Data Replication Interface (DRI). DRI should be a standard-based interface implemented by services providing storage functionality. It can be then used by services providing replication or synchronization functionality. It differs from DAI in that it must provide information about change in data from multiple points in time related to previous interaction. That is to efficiently support frequent and often small updates, while full set of data would be rarely required.
- Data Migration Interface (DMI). DMI should be a standard-based interface implemented by services providing storage functionality. It can be then used by either specialized migration services or directly by other storage services. This interface must provide data in an easily exchangeable (or transformable) format so that it can be easily understood. That is in contrast with DAI and DRI where focus would be on size efficiency of data format. A simple example of such two fromats might be XML vs. JSON.
- Data Tunneling Interface (DTI). DTI should be a standard-based interface implemented by services that would provide tunneling functionality used by processing functionality to tunel DAI interactions.

The data management interfaces should allow basic security services integration and consistent security context management. Although, they are not enough to support accountability and trust among services, they might serve as a basis for such solutions.

IV. SECURITY SERVICES LIFECYCLE MANAGEMENT

The proposed architectural model for on-demand infrastructure services provisioning should rely on the well-defined services lifecycle management (SLM) model and corresponding supporting infrastructure.

We refer in this paper to the Security Services Lifecycle Management (SSLM) model proposed by authors in earlier work [20]. The SSLM describes security services operation in generically distributed multidomain environment and extends the existing SLM frameworks (and SDF in particular) with the additional stages "Reservation Session Binding" (as part of the SDF reservation stage) and "Registration and Synchronisation" (as part of the SDF deployment stage), which specifically target such scenarios as the provisioned services/resources restoration, upgrade or migration (in the framework of the active provisioning session) and provide necessary mechanisms for remote data protection by binding them to the provisioning session context and remote run-time environment.

To ensure integrity of the service lifecycle management, the consistent services context management mechanisms should be defined and used during the whole service lifecycle. In particular case of the security services, the security services should ensure integrity/continuity of the service context management together with ensuring integrity of the security context itself along the services lifecycle and multiple actors and component services. Important role in this process belongs to dynamic security associations that should be supported by dynamic trust anchors binding to the Cloud virtualisation platform runtime environment and special bootstrapping procedure or protocol. However, it is perceived that implementing such functionality will require the service hosting platform that supports Trusted Computing Platform Architecture (TCPA) [24, 25].

V. DYNAMICALLY PROVISIONED ACCESS CONTROL INFRASTRUCTURE (DACI)

Developing a consistent framework for dynamically provisioned security services requires deep analysis of all underlying processes in the main infrastructure or application. Many processes typically used in traditional security services infrastructure need to be abstracted, decomposed and formalized. First of all it is related to the security services setup, configuration and security context management that in many present solutions/frameworks is provided manually, during the service installation or configured out-of-band.

The proposed security framework for on-demand provisioned infrastructure services should address two general aspects: supporting secure operation of the provisioning infrastructure what is typically provided by the providers Authentication and Authorisation Infrastructure (AAI) supported also by the Federated Identity Management services (FIdM), and provisioning a dynamic access control infrastructure (DACI) as part of the provisioned on-demand virtual infrastructure. The first task is primarily focused on the security context exchanged between involved services, resources and access control services. The virtualised DACI should be dynamically linked to the provisioned on-demand VI and VIP trust domains as an entity participated in the handling initial request for VI and legally and securely bound to the VI users. Such security bootstrapping can be done at the deployment stage.

Virtual access control infrastructure setup and operation is based on the mentioned above dynamic security association DSA that will link the VI dynamic trust anchor(s) with the main actors and/or entities participating in the VI provisioning – VIP and the requestor or target user organisation (if they are different). As discussed above, the creation of such DSA for the given VI can be done during the reservation and deployment stage. Reservation stage will allow to distribute the provisioning session context and collect the security context (e.g. public key certificates) from all participating infrastructure components. The deployment stage can securely distribute either shared cryptographic keys or another type of security credentials that will allow validating information exchange and apply access control to VI users, actors, services.

Figure 2 illustrates in details interaction between main actors and access control services during the reservation stage and other stages of provisioned infrastructure lifecycle. The request to create VI (RequestVI) initiates a request to VIP that will be evaluated by VIP-AAI against access control policy, what next will be followed by VIP request to PIP for required or selected physical resources PR's, which in its own turn will be evaluated by PIP-AAI. It is an SDF and SSLM requirements that starting from the initial

RequestVI all communication and access control evaluations should be bound to the provisioning session identifier GRI. The chain of requests from the User to VIO, VIP and PIP can also carry corresponding trust anchors TA0…TA2, e.g. in a form of public key certificate (PKC) [26] or WS-Trust security tokens [27].

DACI is created at the deployment stage and controls access to and use of the VI resources, it uses dynamically created security association of the users and resources. The DACI bootstrapping can be done either by fully pre-configuring trust relations between VIP-AAI and DACI or by using special bootstrapping registration procedure similar to those used in TCPA.

To ensure unambiguous session context and all involved entities and resources identification the following types of identifiers are used:

- Global Reservation ID (GRI) – generated at the beginning of the VI provisioning, stored at VIO and returned to User as identification of the provisioning session and the provisioned VI.
- VI-GRI – generated by VIP as an internal reservation sessions ID, which can be also re-folded GRI depending on VIP provisioning model.
- PR-LRI and VR-LRI – provide identification of the committed or created PR@PIP and VR@VIP.

In the proposed DACI we re-use the authorisation tokens as a session context management mechanisms initially proposed by authors in the GAAA-NRP and used for authorisation (AuthZ) session context management in multi-domain network resource provisioning [28]. Tokens as session credentials are abstract constructs that refer to the related session context stored in the provisioned resources or services. The token should carry session identifier, in our case GRI or VI-GRI.

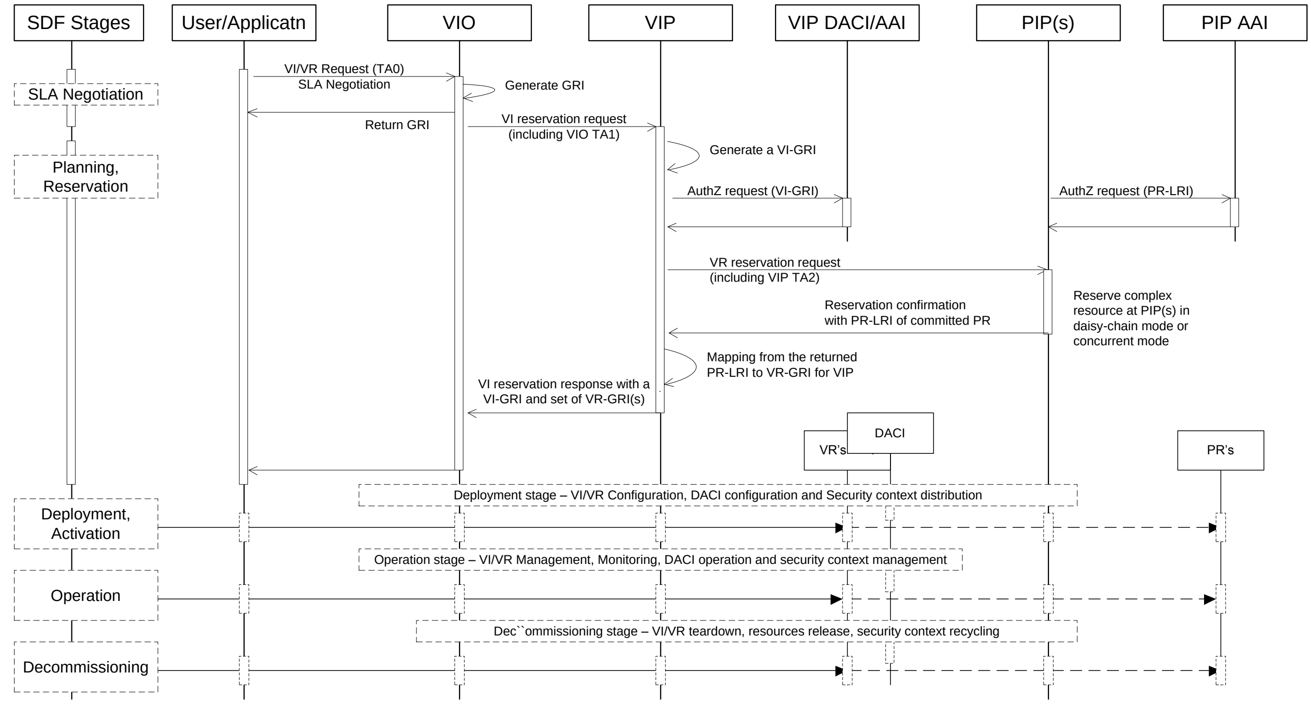

Figure 2. Security context management during the VI provisioning and operation.

In the discussed DACI architecture the tokens are used both for access control and signaling at different SDF/SSLM stages as a flexible mechanism for communicating security context between administrative and security domains (that may represent PIP or individual physical resources). Inherited from GAAA-NRP the DACI uses two types of tokens:

- Access tokens that are used as AuthZ/access session credentials and refer to the stored reservation context.
- Pilot tokens that provide flexible functionality for managing the AuthZ session during the Reservation stage and the whole provisioning process.

AuthZ token serves as a common container for communicating general security context SecCtx between all components of the provisioning infrastructure and provisioned infrastructure instance.

When requesting VI services or resources at the operation stage, the requestor need to include the reservation session credentials together with the requested resource or service description which in its own turn should include or be bound to the provisioned VI identifier in a form of GRI or VI-GRI. The DACI context handling service should provide resolution and mapping between the provided identified and those maintained by the VIP and PIP, in our case VR-LRI or PR-LRI. If session credentials are not sufficient, e.g. in case when delegation or conditional policy decision is required, all session context information must be extracted from authorisation token and the normalised policy decision request will be sent to the DACI Policy Decision Point (PDP) which will evaluated the request against the applied access control policy.

VI. SLA MANAGEMENT

SLA is an important component and a mechanism in virtualised Cloud infrastructure services provisioning and management that creates initial framework/basis for the relations between all major actors in Cloud based services delivery and operation (including provider, operator, broker, customer, end user, etc.). Current practice in provisioning Cloud resources is mostly based on the static Service Level Agreement (SLA) that also describes security measures taken by the provider but doesn't define mechanisms for checking them by users.

In contrast, we propose an approach that requires from the provider to provide interfaces to verify the QoS and other SLA related conditions and obligations during run-time in order to determine whether a guarantee related to a QoS term is fulfilled or violated.

The SLA document defines the requested infrastructure services parameters containing also QoS operation criteria and may also include SLA negotiation process. The SLA is based on templates that expose the QoS a provider is willing to deliver to its customers. Besides QoS parameters related to infrastructure parameters like speed of computer processing units (CPU), memory, network connectivity between CPUs. These templates also include specific security parameters defining the requirements to the security infrastructure and related security context (such as trusted certificate or key serving as initial trust anchor TA0, session based context, etc.) that may be used for defining initial trust relations, i.e. security association, between user/customer and provider.

The necessary functionality for building infrastructure for creating and managing service level agreements will be provided by the WSAG4J framework [29]. WSAG4J is a full implementation of the Open Grid Forum's recommendation WS-Agreement [30]. Besides the protocol defined in WS-Agreement v1.0 it also provides an implementation the current draft specification for a protocol allowing more sophisticated negotiations on top of WS-Agreement. WSAG4J provides comprehensive support for common SLA management tasks such as SLA template management, SLA negotiation and creation, and SLA monitoring and accounting. The negotiation and creation of SLAs is based on templates that expose the quality of service a service provider is willing to provide to a customer. As depicted in Figure 3 the contents of these templates can be modified during the process of SLA creation and negotiation (within constraints defined by the service provider) to better match the requirements of a customer.

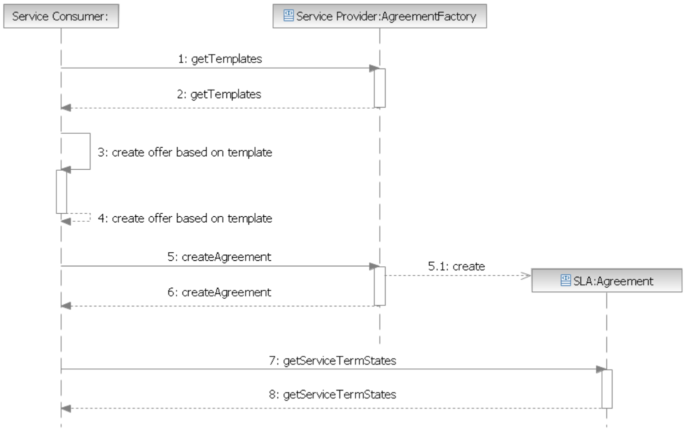

Figure 3. SLA creation and monitoring using the WS-Agreement protocol.

More comprehensive SLA management may require using of the Semantic Web technologies and using ontologies for SLA definition and logical reasoning as discussed in [31] and applied for inter-cloud scenario by Wlodarczyk in [32].

VII. IMPLEMENTATION SUGGESTIONS

When considering DACI implementation as a new approach to the virtualised security services provisioning and management, we can build it using the previous development by the authors the GAAA-NRP profile [33] that implements the generic AAA Authorisation framework [34] for Network Resources Provisioning (NRP). The GAAA-NRP provides rich functionality for authorisation session context management for multidomain network resources provisioning, in particular using access and pilots tokens for access control and signaling. Extending GAAA-NRP to support the proposed DACI for on-demand infrastructure services provisioning will require adding special functionality for security services lifecycle management and in particular to support additional stages related to infrastructure services deployment and provide flexible policy management for DACI. First of all, it is related to the definition of the Common Security Services Interface.

A. *Common Security Services Interfaces (CSSI)*

WS-Security standard, as native to SOA and ESB [16, 17], provides necessary security mechanisms and interface for virtualised resources interconnection, but their practical use in multi-domain/inter-domain virtualised environment will be complicated with necessary configuration of the trust relations and namespaces at each communicating entity. The CSSI has been proposed to simplify communication and configuration of the dynamically provisioned virtualised security services. Technically CSSI combines the core functionality of the GSS-API [35] for authentication service, GAAA-NRP authorisation and session/token management [33]. The CSSI can be used together with WS-Security but introduces a simplified CSSI request format and SOAP security header structure that uses a common SecurityContext container with the following structure:

```
SecurityContext (AuthenticationData,
   AuthorisationData, SessionData, SecurityData)
```

Such approach will allow more flexibility in defining actual security data format and semantics that will be exchanged between the virtualised services and the provider services, which due to their dynamicity will have high variation of the structure and semantics. CSSI and DACI will be configured together with provisioned VI at the deployment stage.

B. Authorisation Session Context Management in the GAAA Toolkit

The required DACI functionality is being implemented based on the GAAA Toolkit (GAAA-TK) pluggable Java library in the framework of the GEYSERS project [13]. The GAAA-TK implements the basic AAA Authorisation framework functionality [34] and extends it with the authorisation session security context management functionality that uses authorisation tickets and tokens as session credentials.

One of the key functional components to support AuthZ session management using AuthzTokens as session credentials is the Token Validation Service (TVS). It is implemented as a part of the general GAAA-TK library but can also be used separately and integrated into other AuthZ frameworks.

The GAAA TK library provides few Policy Enforcement Point (PEP) and TVS methods that support extended AuthZ session management and provide necessary AuthZ tokens and tickets handling functionality (refer to the GAAA-TK release documentation [33] for the complete API description).

The GAAA-TK is extended with the CSSI functionality and the proposed SSLM security mechanisms to support consistent services lifecycle management [14], and flexible configuration functionality to support complex multidomain resource provisioning.

VIII. SUMMARY AND FUTURE DEVELOPMENT

This paper presents the ongoing research on developing architecture and framework for dynamically provisioned security services as part of the provisioned on-demand infrastructure services to support modern e-Science and high-technology industry applications that require both high-performance computing resources and high-speed dedicated transport network.

The paper refers to the generalised model for provisioning infrastructure services on demand and discusses conceptual issues in provisioning consistent security services as a part of the general service provisioning.

The paper analyses general use case and abstract model for on-demand infrastructure services provisioning, identifies required security mechanisms and infrastructure services to support and build consistent security services provisioned on-demand. The suggestions are also provided for dynamic SLA management using Web Services Agreement standard and Cloud data security services implementation.

The paper proposes the Dynamically provisioned Access Control Infrastructure (DACI) architecture and provides the general implementation suggestions for the security context management mechanisms that can be used in the dynamically provisioned access control infrastructure. The paper refers to the existing implementation of the GAAA Toolkit library that provides reach functionality for authorisation session context management with authorisation tickets and tokens.

The proposed DACI and its component functionalities are currently being developed in the framework of the two EU projects GEYSERS and GEANT3. One of current research directions is to propose the virtual security infrastructure bootstrapping mechanism that would allow binding the virtual infrastructure security context to the Cloud virtualisation platform runtime environment.

The presented research is planned to be contributed to the recently created the Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) [36], where the authors play active role.

The authors believe that concepts proposed in this paper will provide a good basis for further discussion among researchers about defining architectural models for dynamically provisioned virtualised security services as part of the general on-demand infrastructure services provisioning.

ACKNOWLEDGEMENTS

This work is supported by the FP7 EU funded project GEANT3 (FP7-ICT-238875), and the FP7 EU funded Integrated project The Generalised Architecture for Dynamic Infrastructure Services (GEYSERS, FP7-ICT-248657).

REFERENCES

[1] NIST SP 800-145, “A NIST definition of cloud computing”, [online] Available: http://csrc.nist.gov/publications/drafts/ 800-145/Draft-SP-800-145_cloud-definition.pdf

[2] GFD.150 Using Clouds to Provide Grids Higher-Levels of Abstraction and Explicit Support for Usage Modes. [Online]. http://www.ogf.org/documents/GFD.150.pdf

[3] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, December 2009. http://www.cloudsecurityalliance.org/csaguide.pdf

[4] Cloud Computing: Benefits, risks and recommendations for information security, Editors Daniele Catteddu, Giles Hogben, November 2009. http://www.enisa.europa.eu/ act/rm/files/deliverables/cloud-computing-risk-assessment

[5] Securing the Cloud: Designing Security for a New Age, Dec. 10, 2009. [Online] http://i.zdnet.com/whitepapers/ eflorida_ Securing_Cloud_Designing_Security_New_ Age.pdf

[6] Amazon AWS Security Center. Certification and Accreditation. [Online] http://aws.amazon.com/security/#certifications

[7] Amazon Boosts Web Services Security for Government Agencies. PCWorld Business Center. April 17, 2011. [Online] http://www.pcworld.com/businesscenter/article/238276/amazon_boosts_web_services_security_for_government_agencies.html

[8] 8. Kaufman, C., R. Venkatapathy. Windows Azure Security Overview. [Online] http://download.microsoft.com/download/6/0/2/6028B1AE-4AEE-46CE-9187-641DA97FC1EE/Windows%20Azure%20 Security%20 Overview%20v1.01.pdf

[9] SAML Single Sign-On (SSO) Service for Google Apps. [Online] http://code.google.com/googleapps/domain/sso/saml_reference_implementation.html

[10] Demchenko Y., A. Mavrin, C. de Laat, "Defining Generic Architecture for Cloud Infrastructure as a Service Provisioning model", CLOSER2011 Conference, 7-9 May 2011, Nordwijk, Netherlands.

[11] Generic Architecture for Cloud Infrastructure as a Service (IaaS) Provisioning Model, Release 1. SNE Techn. Report SNE-UVA-2011-03, 15 April 2011. [Online] http://staff.science.uva.nl/~demch/ worksinprogress/sne2011-techreport-2011-03-clouds-iaas-architecture-release1.pdf

[12] GEANT Project. [Online] http://www.geant.net/pages/home.aspx

[13] Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project). [Online] http://www.geysers.eu/

[14] Demchenko, Y., D.R. Lopez, J.A. Garcia Espin, C. de Laat, "Security Services Lifecycle Management in On-Demand Infrastructure Services Provisioning", International Workshop on Cloud Privacy, Security, Risk and Trust (CPSRT 2010), 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom2010), 30 November - 3 December 2010, Indianapolis, USA.

[15] TMF Service Delivery Framework. [Online] http://www.tmforum.org /servicedeliveryframework/4664/home.html

[16] OASIS Reference Architecture Foundation for Service Oriented Architecture 1.0, Comt. Draft 2, Oct. 14, 2009. [Online] http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-cd-02.pdf

[17] Chappell, D., "Enterprise service bus", O'Reilly, June 2004. 247 pp.

[18] OSGi Service Platform Release 4, Version 4.2. - http://www.osgi.org/Download/Release4V42

[19] Globus Provision. [Online] Available: http://www.globus.org/provision/

[20] Demchenko, Y., C. de Laat, O. Koeroo, D. Groep, "Re-thinking Grid Security Architecture". Proceedings of IEEE Fourth eScience 2008 Conference, December 7–12, 2008, Indianapolis, USA. Pp. 79-86. IEEE Computer Society Publishing. ISBN 978-0-7695-3535-7 / ISBN 978-1-4244-3380-3.

[21] GFD.80 "The Open Grid Services Architecture, Version 1.5", I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R. Subramaniam, J. Treadwell, J. Von Reich. Open Grid Forum, September 5, 2006.

[22] Zhao, G., C. Rong, J. Li, F. Zhang, Y. Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers," IEEE International Conference on Cloud Computing Technology and Science, November 30-December 03, Indianapolis, Indiana. pp. 97-103. ISBN: 978-0-7695-4302-4.

[23] Zhao, G., C. Rong, M. Jaatun, F. Sandnes, "Reference deployment models for eliminating user concerns on cloud security", The Journal of Supercomputing, Published Online 17 June 2010. DOI: 10.1007/s11227-010-0460-9

[24] Demchenko Y., F. Siebenlist, L. Gommans, C. de Laat, D. Groep, O. Koeroo, "Security and Dynamics in Customer Controlled Virtual Workspace Organisation," Proc. HPDC2007 Conference, Monterey Bay California, June 27-29, 2007.

[25] Trusted Computing Group (TCG). [Online]. Available: https://www.trustedcomputinggroup.org/home

[26] RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008. [Online] http://www.ietf.org/rfc//rfc5280

[27] Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). OASIS Standard Specification, 1 February 2006. [Online] http://www.oasis-open.org/committees/download.php/ 16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[28] Demchenko, Y., M. Cristea, C. de Laat, E. Haleplidis, Authorisation Infrastructure for On-Demand Grid and Network Resource Provisioning, Proceedings Third International ICST Conference on Networks for Grid Applications (GridNets 2009), Athens, Greece, 8-9 September 2009. ISBN: 978-963-9799-63-9

[29] WSAG4J – WS-Agreement framework for java. February 2011. [Online] http://packcs-e0.scai.fraunhofer.de/wsag4j/

[30] WS-Agreement specification. Open Grid Forum GFD.107. May 2008. [Online] http://www.ogf.org/documents/GFD.107.pdf

[31] Fakhfakh, K., T. Chaari, S. Tazi, K. Drira, M. Jmaiel, "A Comprehensive Ontology-Based Approach for SLA Obligations Monitoring,", The 2nd Int. Conf. on Advanced Engineering Computing and Applications in Sciences, 2008. pp. 217-222,.

[32] Wlodarczyk, T., C. Rong, K. Thorsen, "Industrial Cloud: Toward Inter-enterprise Integration", Proceedings of the 1st International Conference on Cloud Computing (CloudCom '09), Springer-Verlag, Berlin, Heidelberg, 460-471.

[33] "GAAA Toolkit pluggable components and XACML policy profile for ONRP", Phosphorus Project Deliverable D4.3.1. – September 30, 2008. [Online]. Available: http://www.ist-phosphorus.eu/files/ deliverables/Phosphorus-deliverable-D4.3.1.pdf

[34] RFC 2904 - "AAA Authorization Framework" J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, August 2000 - ftp://ftp.isi.edu/in-notes/rfc2904.txt

[35] RFC2853 - Generic Security Service API Version 2 : Java Bindings. June 2000. [Online] http://www.ietf.org/rfc/rfc2853.txt

[36] Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG). [Online]. http://www.ogf.org/gf/event_schedule/index.php?event_id=17