Access Control Infrastructure for On-Demand Provisioned Virtualised Infrastructure Services

Yuri Demchenko
University of Amsterdam
y.demchenko@uva.nl

Canh Ngo
University of Amsterdam
T.C.Ngo@uva.nl

Cees de Laat
University of Amsterdam
delaat@uva.nl

ABSTRACT

Cloud technologies are emerging as a new way of provisioning virtualised computing and infrastructure services on-demand for collaborative projects and groups. Security in provisioning virtual infrastructure services should address two general aspects: supporting secure operation of the provisioning infrastructure, and provisioning a dynamic access control infrastructure as part of the provisioned on-demand virtual infrastructure. Dynamically provisioned access control infrastructure (DACI) reveals a wide spectrum of problems related to the distributed access control, policy and related security context management. Consistent security services design, deployment and operation require continuous security context management during the whole security services lifecycle, which is aligned to the main provisioned services lifecycle. The paper discusses conceptual issues, basic requirements and practical suggestions for provisioning dynamically configured access control services. The paper discusses security mechanisms that are required for consistent DACI operation, in particular use of authorisation tokens for access control and authorisation session context exchange between infrastructure services and providers. The proposed security infrastructure implementations are based on the GAAA-Toolkit that provides rich security session context management functionality with authorisation tickets and tokens.

KEYWORDS: Dynamic Access Control Infrastructure, Infrastructure Virtualisation, On-Demand Infrastructure Services Provisioning, Security Service Life-cycle Management, Security Context Management.

1. INTRODUCTION

Clouds 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 as 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 Service Level Agreement (SLA) that in general defines mutual provider and user expectations and obligations. However, such approach doesn't scale well with the potential need to combine Cloud based services from multiple providers when building complex infrastructures for collaborative projects and groups.

Cloud providers are investing a lot into making their own infrastructure secure and complying to existing security management industry standards (e.g. Amazon Cloud recently achieved PCI DSS compliance certification [6]), however the overall security of the Cloud based applications and services will depend on two other factors: security services implementation in user applications and binding between virtualised services and Cloud virtualisation platform.

Practical Cloud usage within one provider infrastructure brings illusion about unlimited availability, “elasticity” and “perfect” security, but in practice this is related only to limited range of services and with limited manageability. Currently provided security services are based on VPN security model and provide only simple access control services based on users access over SSH as a commonly used secure channel. 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.

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 presented research is based on previous works by authors that have been resulted in proposing the general Complex Resource Provisioning (CRP) model that was used as a basis for development of the Generic AAA Authorisation infrastructure (GAAA-CRP) [7, 8, 9] for combined Grid and network resources provisioning in the framework of the Phosphorus project [10]. The proposed GAAA-CRP authorisation infrastructure supports the main stages of the CRP process such as reservation, deployment, access, and decommissioning. Current research and development continue in the framework of the GEANT3 [11] and GEYSERS [12] projects and target developing a consistent security services architecture for Infrastructure Services provisioned On-Demand (ISOD). The paper also refers to another paper by authors [13] that describes the ISOD architectural framework used as a basis for developing the proposed security infrastructure.

The paper is organized as follows. Section 2 provides a short reference to the generalised architecture for on-demand infrastructure services provisioning described in [13] and analyses trust relations between physical and virtual resources and infrastructures. Section 3 discusses the security paradigm shift in Cloud Computing and summarises the basic security requirements to the dynamically provisioned security services. Section 4 introduces the proposed Security Services Lifecycle Management (SSLM) model that extends existing service lifecycle management frameworks with additional stages to support on/demand services provisioning. Sections 5 and 6 discuss DACI operations and security context management during the services provisioning stages. Section 7 provides implementation suggestions, and finally, section 8 provides summary and discussed possible further developments.

2. ON-DEMAND INFRASTRUCTURE SERVICES PROVISIONING

The basic use case for provisioning the project or group oriented Virtual Infrastructure (VI) for e-Science that includes both computing resources and supporting network is described in [13]. Figure 1 below presents the abstraction of the VI provisioning process where the VI is provisioned for two collaborative user groups A and B in different locations or campuses. In order to fulfill their tasks (e.g. cooperative image processing and analysis), they 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 example contains all basic components of the typical e-Science research process: data production with scientific instrument (labeled as VI resource node VIR4), initial data mining and filtering (VIR3, VIR5), analysis with special scientific applications (VIR1, VIR6), and finally presentation and visualisation (VIR1, VIR6).
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 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 [13] implements and extends the related TeleManagement Forum SDF definition [14]. 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 Meatadata Service (MD-SL) that maintains VI and component services identifies, stages, versions and binds them to the SLA and provisioning sessions IDs.

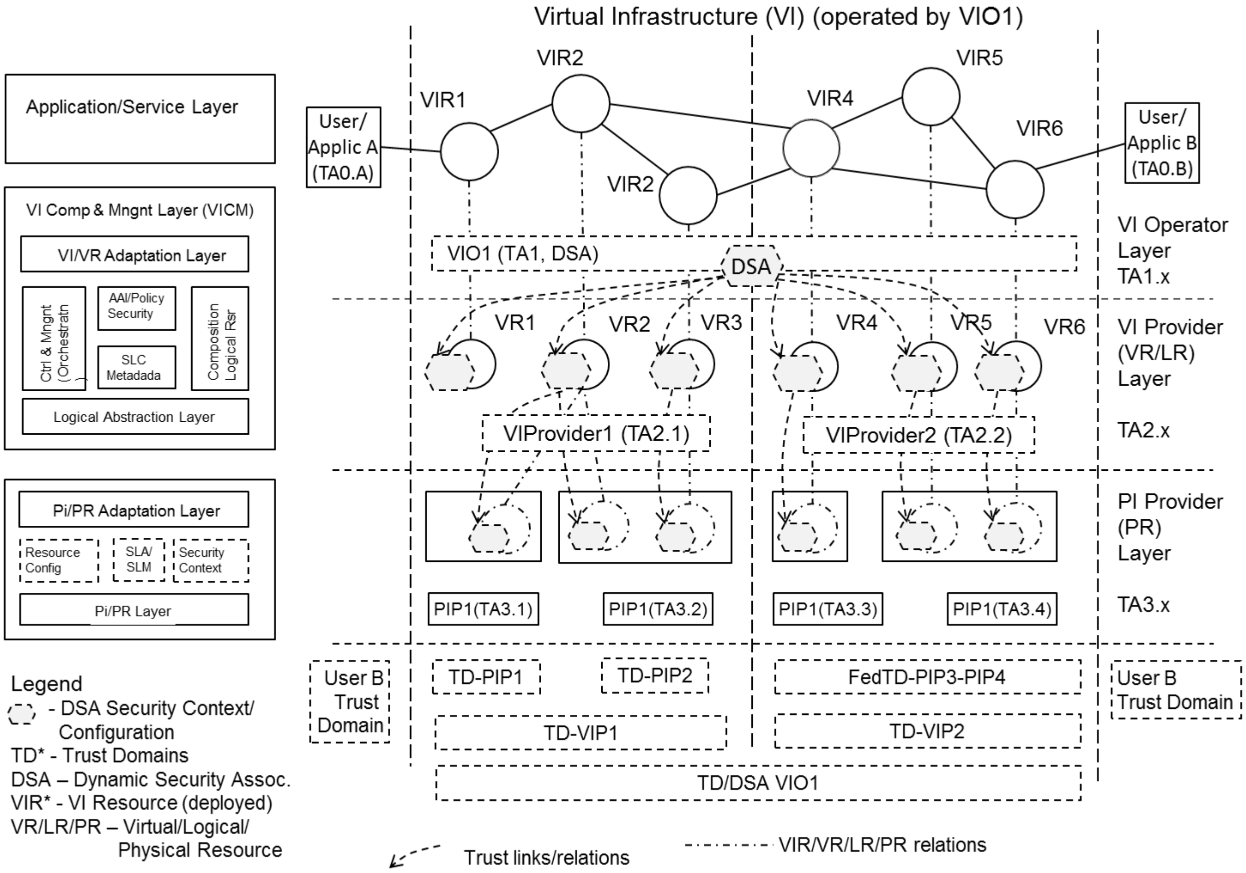

Figure 1. Main actors, functional layers and processes in on-demand infrastructure services provisioning.

Physical Resources (PR) in order to be included into VI composition and provisioning by the VIP need to be abstracted to the Logical Resources (LR) that will undergo a number of abstract transformations to compose a required VI. The VI comprising LR's need to be deployed to the PIP as 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 initialisation, 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.

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 allowing to define a common access control policies. Access decision made at the VI/VIO level should be trusted and validated at the PR/PIP level, what is 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) [15] 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 [16, 17].

3. GENERAL REQUIREMENTS TO DYNAMICALLY PROVISIONED SECURITY SERVICES

On-demand provisioning of 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. 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 remaining in 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 trust and security model [18, 19]. In general, the VO based environment is considered as trusted.

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 resource. 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 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 the traditional confidentiality, integrity, access control services, also data lifecycle management and synchronization.
- Access control infrastructure virtualisation and dynamic provisioning, including dynamic/automated access control policies generation or composition.
- Security services lifecycle management, in particular service related metadata and properties, and their binding to the 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.
- Trust and key management in provisioned on demand security infrastructure, and support of the Dynamic Security Associations (DSA) that should provide fully verifiable chain of trust from the user client/platform to the virtual resource and the virtualisation platform.
- SLA management, including initial SLA negotiation, SLA enforcement at the planning stage and SLA monitoring at the operation stage. SLA can specify security requirements and trust anchors that can be used for bootstrapping the DSA at the provisioning stages.

The security solutions and supporting infrastructure should support consistent security sessions management:

- Special session for data transfer that should also support data partitioning and run-time activation and synchronization.
- 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.

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

4. 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. Most of existing SLM frameworks and definitions are oriented on rather traditional human-driven services development and management. The SOA based Service Delivery Framework (SDF) by TMF provides a good basis for defining the general services lifecycle management framework that includes both the basic service delivery stages and necessary supporting infrastructure services [16]. Dynamically provisioned and re-configured services will require re-thinking existing models and proposing new security mechanisms at each stage of the typical provisioning process.

Figure 2 illustrates the proposed Security Services Lifecycle Management (SSLM) in relation to the general services lifecycle model that reflects security services operation in generically distributed multi-domain environment and their binding to the provisioned services and/or infrastructure [20]. The SSLM includes the following stages:

- Service request and generation of the Global Reservation ID (GRI) that will serve as a provisioning session identifier and will bind all other stages and related security context.

- Reservation session binding that provides support for complex reservation process including required access control and policy enforcement.
- Deployment stage that begins after all component resources have been reserved and includes distribution of the security context and binding the reserved resources or services to the GRI.
- Registration&Synchronisation stage that may include also special procedure for trust anchors bootstrapping. It specifically addresses possible scenarios with the provisioned services migration or failover.
- During Operation stage the security services provide access control to the provisioned services and maintain the service access or usage session.
- Decommissioning stage ensures that all sessions are terminated, data are cleaned up and session security context is recycled.

Table 1 also explains what main processes/actions take place during the different SLM/SSLM stages and what general and security mechanisms are used, in particular:

- SLA that defines that requested infrastructure services parameters containing also QoS operation criteria; may also include SLA negotiation process.
- Workflow that may be used at the Operation stage as service Orchestration mechanism and can be originated from the design/reservation stage.
- Metadata that are created and used during the whole service lifecycle and together with security services actually ensure the integrity of the SLM/SSLM.
- Dynamic security associations (DSA) that support the integrity of the provisioned resources and are bound to the security sessions.
- Authorisation session context that supports integrity of the authorisation sessions during Reservation, Deployment and Operation stages.
- Logging can be actually used at each stage and essentially important during the last 2 stages – Operation and Decommissioning.

The proposed SSLM model extends the existing SLM frameworks and earlier proposed by authors the CRP model [8] with the additional stages “Reservation Session Binding” and “Registration & Synchronisation” which especially target such scenarios as the provisioned services/resources restoration, re-planning or migration (in the framework of the active provisioning session) and provide a mechanism for remote data protection by binding them to the session context. Important role in these processes belongs to the consistent security context management and dynamic security associations that should be supported by dynamic trust anchors binding 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) [21, 22].

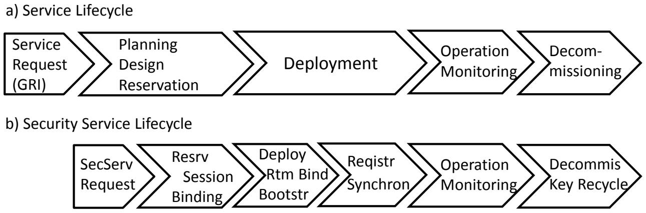

Figure 2. The proposed Security Services Lifecycle Management model.

Table 1. Relation between SSLM stages and supporting security mechanisms

SLM stages	Request	Planning Reserve	Deploy	Operation	Decommis-sioning
SSLM Process/ Activity	SLA Negotiation	Serv/Rsr Compose Reserve	Configure Bootstrap Synchron	Orchestration/ Session Management	Logoff Accounting
Supporting Mechanisms (M – mandatory, O - optional)					
SLA	M				O
Workflow		O		M	
Metadata	M	M	M	M	
Dynamic Security Associatn		O	M	M	
AuthZ SecCtx		M	M	M	
Logging		O	O	M	M

5. DYNAMICALLY PROVISIONED ACCESS CONTROL INFRASTRUCTURE (DACI)

Developing a consistent framework for dynamically provisioned security services requires deep analysis of all underlying processes and interactions. 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 general security framework for on-demand provisioned infrastructure services should address two general aspects: (1) 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 (2) 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 must be bootstrapped to the provisioned on-demand VI and VIP/VIO trust domains as entities participating 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 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 initial 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 3 illustrates in details interaction between main actors and access control services during the reservation stage and includes also 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) [23] or WS-Trust security tokens [24].

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 [22].

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.

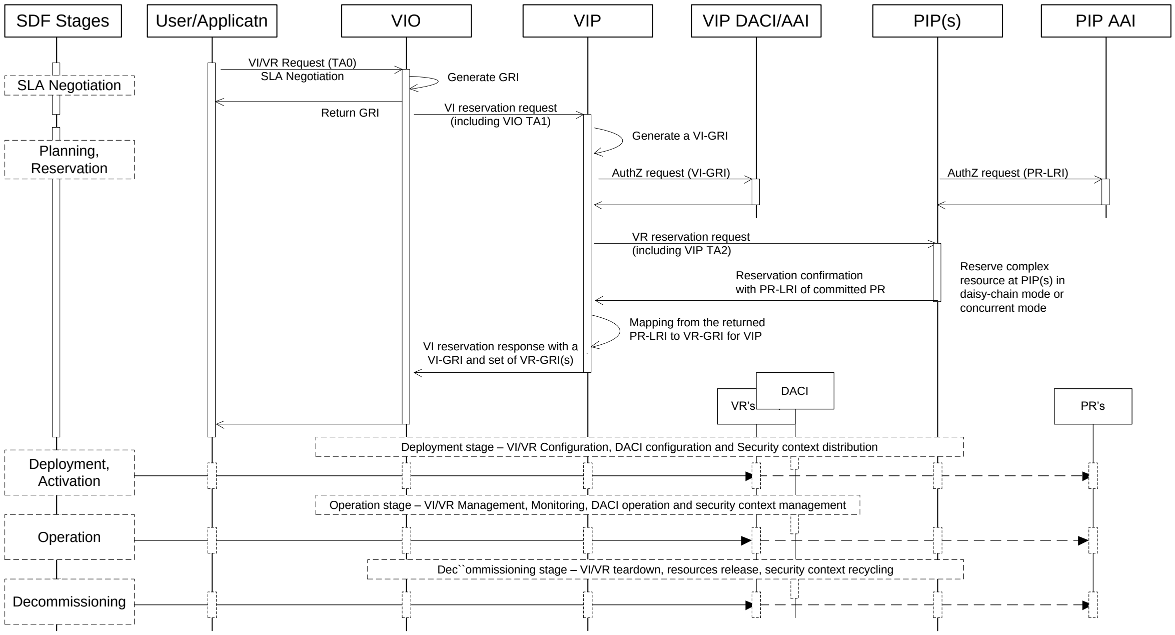

Figure 3. Security context management during the VI provisioning and operation

6. SECURITY CONTEXT MANAGEMENT IN DACI

Although DACI operates at the Operation stage, its security context is bound to the overall provisioning process starting from SLA negotiation that will provide a trust anchor TA0 to User/application security domain with which the DACI will interact during the Operation stage. The RequestVI initiates the provisioning session inside of which we can also distinguish two other types of sessions: reservation session and access session, which however can use that same access control policy and security context management model and consequently can use the same format and type of the session credentials. In the discussed DACI we re-use the authorisation (AuthZ) tokens (AuthzToken) mechanism initially proposed in the GAAA-NRP and used for authorisation session context management in multi-domain network resource provisioning [8, 25]. 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.

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 identifiers 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 AuthzToken and the normalised policy decision request will be sent to the DACI Policy Decision Point (PDP) which will evaluate the request against the applied access control policy.

In the discussed DACI architecture the tokens are used both for access control and signaling at different SSLM/SDF stages as a flexible mechanism for communicating and signaling 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.

Figure 4 illustrates the common data model of both access token and pilot token. Although the tokens share a common data-model, they are different in the operational model and in the way they are generated and processed. When processed by the AuthZ service components they can be distinguished by the token type attribute which is optional for access token and mandatory for pilot token.

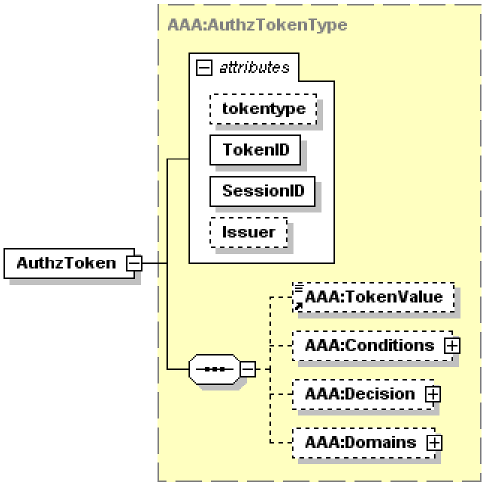

Figure 4. Common access and pilot token datamodel

Access tokens contain three mandatory elements: the SessionId attribute that holds the GRI; the TokenId attribute that holds a unique token ID attribute and is used for token identification and authentication; and the TokenValue element. The optional elements include: the Condition element that may contain two time validity attributes notBefore and notOnOrAfter; the Decision element that holds two attributes ResourceId and Result; and optional element Obligations that may hold policy obligations returned by the PDP. Pilot token may contain another optional Domains element that serves as a container for collecting and distributing domain related security context.

For the purpose of authenticating token origin, the pilot token value is calculated of the concatenated strings "DomainId, GRI, TokenId". This approach provides a simple protection mechanism against pilot token duplication or replay during the same reservation/authorisation session. The following expressions are used to calculate the TokenValue for the access token and pilot token:

```
TokenValue = HMAC(concat(DomainId, GRI, TokenId),
TokenKey)
```

In the current implementation, the TokenKey is generated from the GRI and a common shared secret value among all trusted domains. It means that only these domains can generate valid tokens and correspondingly verify the authenticity of the received tokens. The shared secret can be distributed as a part of the DSA creation. It is also suggested all participating resources and/or domains cache received tokens and checks their uniqueness.

7. IMPLEMENTATION SUGGESTIONS

The DACI implementation is based on the previous development by authors of the GAAA-NRP profile for Network Resources Provisioning (NRP) in the Phosphorus project [10] that extends the generic AAA Authorisation framework [26] with rich authorisation session context management functionality for multidomain network resources provisioning, in particular, using access and pilots tokens for access control and signaling. Extending GAAA-NRP to support the required DACI functionality for on-demand infrastructure services provisioning will require adding special functionality for security services lifecycle management.

7.1. Common Security Services Interfaces (CSSI)

Native to SOA and ESB [15, 16] the WS-Security framework [24] 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 the necessary namespaces and trust relations configuration at each communicating entity. The CSSI provides a simplified protocol and a Request/Response messages format what should simplify the dynamically provisioned virtualised security services integration with other infrastructure services and applications. Technically CSSI combines the core functionality of the GSS-API [27] for authentication service, GAAA-NRP authorisation service and adds special functionality for session management. The CSSI can be used together with WS-Security by introducing a simplified SOAP security header structure that uses a common SecurityContext container for all security calls with the following structure:

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

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

7.2. 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 developed in the framework of the Phosphorus project. The GAAA-TK implements the basic AAA Authorisation framework functionality and extends it with the authorisation session management functionality that uses authorisation tickets and tokens as session credentials. The GAAA TK library provides few 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 [25] for the complete API description).

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 is extended with the CSSI functionality and the proposed SSLM security mechanisms to support consistent services lifecycle management, and flexible configuration functionality to support complex multidomain resource provisioning.

8. 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.

The paper proposes 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. It is an intension that the proposed model should be further developed to support the Cloud Infrastructure as a Service provisioning model.

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 proposed Security Services Lifecycle Management (SSLM) model addresses specific for on-demand infrastructure service provisioning security problems that require security services synchronization and binding to virtualisation platform and runtime environment. The paper proposes the Dynamically provisioned Access Control Infrastructure (DACI) architecture and defines the necessary security mechanisms to ensure consistent security services operation in the provisioned virtual infrastructure.

The paper provides implementation suggestions for the security context management mechanisms that can be used in the dynamically provisioned access control infrastructure and refers to the existing implementation of the GAAA Toolkit library that provides reach functionality for authorisation session context management.

The proposed DACI and its component functionalities are currently being developed in the framework of the two EU projects GEYSERS and GEANT3.

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

ACKNOWLEDGEMENT

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] 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

[2] NIST Cloud Computing Definition. [Online]. http://csrc.nist.gov/groups/SNS/cloud-computing/

[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. - http://aws.amazon.com/security/#certifications

[7] Demchenko Y, A. Wan, M. Cristea, C. de Laat, "Authorisation Infrastructure for On-Demand Network Resource Provisioning," Proc. 9th IEEE/ACM Int. Conference on Grid Computing (Grid 2008), Tsukuba, Japan, Sept. 29 - Oct. 1, 2008. pp. 95-103. ISBN 978-1-4244-2579-2.

[8] 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

[9] Demchenko, Y., C. M. Cristea, de Laat, XACML Policy profile for multidomain Network Resource Provisioning and supporting Authorisation Infrastructure, IEEE Int. Symposium on Policies for Distributed Systems and Networks (POLICY 2009), July 20-22, 2009, London, UK. ISBN-13: 978-0-7695-3742-9. Pp. 98-101.

[10] Phosphorus Project. [Online]. Available: http://www.ist-phosphorus.eu/

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

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

[13] Demchenko, Y., J. van der Ham, M. Ghijsen, M. Cristea, V. Yakovenko, C. de Laat, "On-Demand Provisioning of Cloud and Grid based Infrastructure Services for Collaborative Projects and Groups", The 2011 International Conference on Collaboration Technologies and Systems (CTS 2011), May 23-27, 2011, Philadelphia, Pennsylvania, USA (This proceedings)

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

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

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

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

[18] 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.

[19] GFD.80 "The Open Grid Services Architecture, Version 1.5". Open Grid Forum, September 5, 2006.

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

[21] Demchenko Y., Frank Siebenlist, Leon Gommans, Cees de Laat, David Groep, Oscar Koeroo, "Security and Dynamics in Customer Controlled Virtual Workspace Organisation," Proc. HPDC2007 Conference, Monterey Bay California, June 27-29, 2007.

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

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

[24] 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

[25] "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

[26] 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

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