OGPX pre BOF	D. Levine, Ed.
Internet-Draft	IBM Thomas J. Watson Research
Intended status: Informational	Center
Expires: January 15, 2010	July 14, 2009

TOC

OGPX layering and architectural patterns
draft-levine-ogp-layering-00

Status of this Memo

Copyright Notice

Abstract

Architectural layering and patterns for OGPX.

Table of Contents

---

1. Requirements Language

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

---

2. Introduction

TOC

This note focuses on design patterns and architectural choices which will permit the OGPX specifications to adapt to a wide range of deployment patterns, within the basic OGXP remit, and support the use of policy to permit the architecture to enable virtual spaces with very different policies toward security, intellectual property, identity, and economics to share common infrastructure and to interoperate in a principled fashion.

This note is preliminary in nature, and is primarily intended to drive a discussion on the specific nature of the requirements for managing diverse deployments, and suppoting diverse policies.

---

3. Mechanisms, Services, Domains, Policy

TOC

When completed, the OGPX specifications will define:

- *a set of underlying service delivery mechanisms
- *a set of services delivered over these mechanisms
- *clusters of related services, called domains
- *mechanisms to apply policy to specific services

The most commonly mentioned partition of services into domains is the split between "agent" and "region" domains proposed by Linden Lab. This partition separates services associated with the user's identity and information, the "agent domain," from services associated with virtual space, the "region domain"
In order to discuss patterns of clustering and service delivery, it is necessary to discuss what is mean by "domain" and also look more deeply into both the notions of a cluster of services, and also discuss possible deployment patterns Servers, Services and Named entities
In order to avoid confusion, in this note, we will define a number of terms very precisely:
Service: a named set of REST style resources which accepts a series of messages to perform a task. We explicitly do not mean a deployed service such as the Second Life(tm) service.
Server: A computer offering up one or more named services
Region: A named portion of virtual space
Agent: The state and services representing a user within the virtual world
Policy: A described behavior of a service within the OGPX specications.

---

4. Deployment patterns

TOC

To motivate the discussion, we will describe several plausible deployment patterns for OGPX based systems. Each of these deployment patterns should be viewed as a use case for the OGPX specifications. The specifications should provide sufficient expresivity of service endpoints, and trust boundaries to support all of the described patterns.

5. Second Life Agent Domain / Region Domain Split

TOC

This deployment pattern represents the pattern Linden Lab proposed in its initial discussions on second generation architecture in 2007. It offloads any services which are not germane to managing a virtual space to an "agent" domain, focused, on the services which are specific, not to the virtual space, but the user's agent.
In this pattern, the viewer is typically connected to one or more regions, and one agent domain. The agent domain acts as a unitary focus for all services associated with the agent. When accessing other services hosted by a deployer other than the hoster of the agent domain, the agent domain acts as the trust source, managing the agent (and user's) access to other regions.
In this deployment pattern, back end services, such as assets and inventory are accessed via the agent domain, do not, inhenrently have thier own event queue or trust domain.

---

6. Standalone OpenSim Region model

TOC

In the Standalone OpenSim deployment model, all of the services comprising a Region, an Agent Domain, and the supporting services used by these services are hosted on a single server. A single event queue may manage connectivity to the services, or several event queues, with the services being hosted as seperate processes within the server. Historically, a standalone OpenSim represents a single fully trusted domain, where there are no seperate trust components or policies.

---

7. OpenSim OGP + Asset reflector + Agent Service

TOC

In this deployment pattern, one or more OpenSim regions are hosted, each as a seperate server. An seperate agent domain acts as the trust authority, and login component for the deployment. Inventory and Asset requests are reflected from individual regions to asset and inventory services, hosted either in a standalone fashion, or as part of an OpenSim region.

TOC

8. OpenSim UGAIM grid model

This is the current (Soon to be deprecated) OpenSim Grid model. In this model, a seperate login service (not an agent domain) is hosted on one server ans a collection of backend services are shared by one or more Region Simulators. The entire grid forms a single trust model.

---

9. Hypergrid

TOC

In this model, each Region is hosted in either Standalone, or UGAIM style Grid mode. Specific links between regions are created, which define a two way mapping, permitting users to move thier avatars between the regions. Service requests related to the back end servcies for these avatars are directed back to the originating service. Trust, if any is established in the process of creating the explicit link between the regions.

---

10. Hypergrid and Cable Beach

TOC

Hypergrid can be combined with cable beach, so that assets are fetched directly from a shared asset server, and trust between the asset server, and between the regions and the user is managed by the client directly.

---

11. Multi-hosted asset deployment

TOC

This is a case in which there are multiple back ends supporting multiple sets of assets. Trust is established either per the Agent Domain model, between services, and the agent's agent domain, or between regions, in hpyergrid fashion, or directly between the client and the asset services, per the cable beach model.

---

12. Factored Service Models

TOC

There is nothing inherent in the requirements of a virtual world deployment that specific back end services be clustered into two domains, nor that a single server or logical endpoint host all of the services which comprise a deployment. Cloud deployed servics may be used to host part or all of a OGPX deployment. In such a deployment

model, services deployed within a cloud may deploy one or more event queue endpoints or service and trust endopints to connect to clients. Factoring of services is not exclusive to back end services, the agent domain, or regions. Deployment models in which regions share services, or in which the services comprising a region are deployed on a distributed computuing fabric should be supported.

---

13. Policy Requirements

TOC

Policy decisions may be made by services on the basis of:

- *End user identity token
- *Requesting Service identity token
- *Service specific token (Proof of license, proof of TOS signature, etc.)

In order to permit policy decisions to be made by services, a number of token may presented to the service. These tokens will likely be supported as optional additions to the protocols, inserted in slots in the protocol messages defined by the services. This permits services to optionally require additional inputs in order to satisfy thier policy requirments in a predictcable and princpled fashion.

---

14. Grid Access authentication

TOC

One policy choice grid deployers may make, is to require a login or authentications to be made to the grid's authentication service or agent domain. Several emerging internet approaches, such as openId or OAuth are possible mechanisms which may be used to satisfy this need.

---

15. IANA Considerations

TOC

This memo includes no request to IANA.

TOC

16. Security Considerations

This draft primarily defines requirements and use cases, as well as a description of policy management approaches. Policy management includes control of choices which affect security. To the extent that requirements and use cases permit poor security choices to be made when deploying services security of a deployed system could be compromised by those considerations.

---

17. References

TOC

17.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

17.2. Informative References

TOC

[cable]	Intel, “Cable Beach Design Wiki,” 2009.
[caps]	Linden Lab, “Open Grid Protocol: Foundation,” 2009.
[intro]	Linden Lab, “Open Grid Protocol: Foundation,” 2009.

Appendix A. Additional Stuff

TOC

This becomes an Appendix.

Author's Address

TOC

	David W. levine (editor)
	IBM Thomas J. Watson Research Center
	19 Skyline Drive
	Hawthorn, New York 10532
	USA
Phone:	+1 914-784-7427
Email:	dwl@us.ibm.com