OSGi Entities

Confidential, Draft
RFC 28

18 Pages

Abstract

The purpose of this document is to provide an overview of the OSGi environment, the actors within, and the definition of their specific roles.

0 Document Information

0.1 Table of Contents

0 Document Information 2
0.1 Table of Contents 2
0.2 Status 3
0.3 Acknowledgement 3
0.4 Terminology and Document Conventions 3
0.5 Revision History 3

1 Introduction 5

2 Motivation and Rationale 5

3 Technical Discussion 6
3.1 Services infrastructure 6
3.1.1 Service Platform 7
3.1.2 Service Platform Server 7
3.1.3 Service Platform Operator 8
3.1.4 Service Application 8
3.1.5 Service User 8
3.1.6 Service Provider 8
3.1.7 Service Deployment Manager 8
3.1.8 Service Operations Support 8
3.2 Additional services infrastructure entities 8
3.2.1 Service Developer 9
3.2.2 Service Aggregator 9
3.2.3 SPS Manufacturer 9
3.2.4 SPS Owner 9

4 Security Considerations 9

5 Examples 10
5.1 Multiple independent service infrastructures 10
5.2 Common service providers 13
5.2.1 Accounting Provider 13
5.2.2 Certification Authority (CA) 13
5.2.3 Gateway Operator 13
5.3 System environment for Service Gateway 14
5.3.1 Service Gateway 15
5.3.2 WAN 15
5.3.3 Local buses & local devices 16
5.3.4 Internet 17
5.3.5 Privacy protected information 17

6 Document Support 17

All Page Within This Box

6.1 References 17
6.2 Author's Address 17
6.3 Acronyms and Abbreviations 18
6.4 End of Document 18

0.2 Status

This document introduces definitions for various entities that are present in an OSGi environment, and requests discussion and suggestions for improvements. Distribution of this document is unlimited within OSGi.

0.3 Acknowledgement

The information contained in this RFC was formed from several team members within and consensus from the Security Expert Group.

0.4 Terminology and Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in [1].

0.5 Revision History

The last named individual in this history is currently responsible for this document.

Revision	Date	Comments
0.1	June 6, 2001	A general overview and description of the OSGi environment and the roles each of the entities performs. Bernard Russell Beland, RFC editor and co-chair for the Security Expert Group.
0.2	Aug 28, 2001	Updated after review in Copenhagen meeting Lars-Erik Helander, Gatespace AB, RFC editor and co-chair for the Security Expert Group.

All Page Within This Box

0.3	Sep 3, 2001	Updated after mail-comments. • Accounting Operator -> Accounting Provider • Picture showing relationship between Bundle/Bundle Object/Bundle File has been removed. • Description about Native OS environment removed. • “RFC xx System model” -> ”RFC 28 OSGi Entities” in document header. Lars-Erik Helander, Gatespace AB, RFC editor and co-chair for the Security Expert Group.
0.4	Oct 18, 2001	New structure. Lars-Erik Helander, Gatespace AB, RFC editor and co-chair for the Security Expert Group.
0.5	Oct 26, 2001	Minor adjustments. Lars-Erik Helander, Gatespace AB, RFC editor and co-chair for the Security Expert Group.
0.6	Nov 29, 2001	Minor updates after TSC review. Lars-Erik Helander, Gatespace AB, RFC editor and co-chair for the Security Expert Group.

All Page Within This Box

1 Introduction

This document is to provide an overall description and system model for the OSGi environment. It also contains the definitions of the entities that act in this environment and their corresponding functions. In addition to this, a number of entities related to generic and specific application domains are also mentioned.

Chapter 3 of this document contains the definitions made this RFC. In addition to this chapter 5 provides a number of examples that are included to provide a better understanding of how the defined terminology could be applied.

2 Motivation and Rationale

This information was originally contained in RFC-18. In an attempt to assign security functions to specific entities it was necessary to define their roles and functions. When this information was shared with other expert groups, it was determined that such information is of global value. It would provide all expert groups with standard definitions from which to proceed.

3 Technical Discussion

3.1 Services infrastructure

This section defines the basic entities related to the service infrastructure. The following entities are defined in this section:

- Service Platform – SP
- Service Platform Server - SPS
- Service Platform Operator - SPO
- Service Application
- Service User
- Service Provider
- Service Deployment Manager - SDM
- Service Operations Support – SOS

It should be noted that additional entities related to the services infrastructure are defined in section 3.2.

The interrelationships between most of these entities are shown in the following figure:

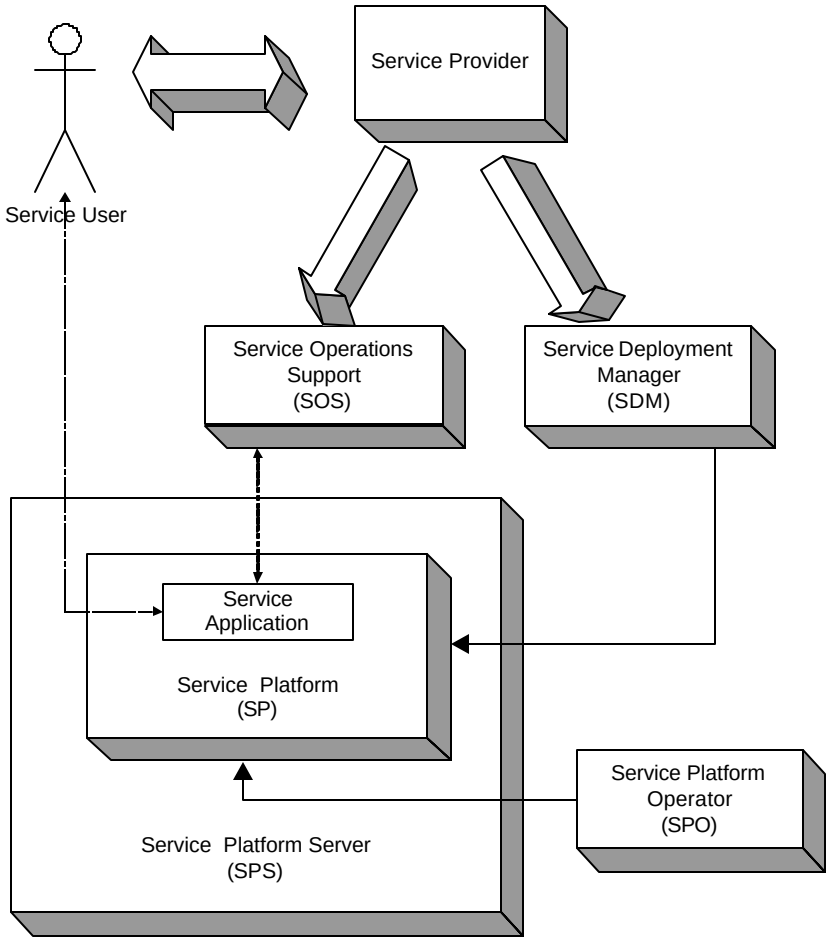

Figure 1: Basic services infrastructure entities

Here follows descriptions of each entity in the figure above. It should be noted that a number of entities are actually roles and one particular person or organisation may take several roles. For example, the same organisation might be Service Provider, Service Platform Operator and Service Deployment Manager.

3.1.1 Service Platform

The basic functionality of the Service Platform is its ability to manage the execution life cycle of service[1] applications. One or more bundles contain the code that is required to perform the tasks of a specific service. The Service Platform is capable of dynamically load/activate/deactivate/update/unload such bundles.

3.1.2 Service Platform Server

The "hardware box" that holds the Service Platform is called the Service Platform Server. The Service Platform Server may be equipped with very specialized hardware suited for its specific application domain. It may house

[1] Note that this is different than the service defined by the service registry within the Service Platform. The service meant here is on a higher level of abstraction.

any number of processors, running Service Platforms and each processor may house any number of Service Platforms.

3.1.3 Service Platform Operator

The main responsibility of the Service Platform Operator is to control who is allowed to deploy services to the Service Platform in question (i.e. control which Service Deployment Managers, see below, that are allowed to operate towards the particular Service Platform. In addition to this he might also manage other functions related to the specific Service Platform instance.

3.1.4 Service Application

A service application is defined to be all bundles in use within a Service Platform that collectively is used to implement a specific service.

3.1.5 Service User

The Service User is defined to be a, possibly human, entity that does at least on of the following:

- Initiate the necessary business events required, in order to ensure that a specific Service Application is created on a specific Service Platform.
- A, possibly human, user that interacts with a specific Service Application during its execution.

The Service Users are end users. They may or may not interact directly with the Service Platform Server as they use it.

3.1.6 Service Provider

The Service Provider represents a business related entity. The Service Provider supplies the necessary means to provide the business related support of a specific service. The Service Provider is also responsible for assigning the tasks of service deployment and service operation management to someone.

3.1.7 Service Deployment Manager

The Service Deployment Manager acts on the behalf of the Service Provider. The SDM manages all issues related to the life cycle of Service Applications.

3.1.8 Service Operations Support

The Service Operations Support acts on behalf of the Service Provider. The SOS is responsible for the systems that interoperate with the Service Applications during their operation. For example, if a Service Application is acting as a Web client towards a specific Web server, the Web server is part of the responsibilities of the SOS.

3.2 Additional services infrastructure entities

In the this section you will find definitions for the following entities:

- Service Aggregator
- Service Developer
- SPS Manufacturer

All Page Within This Box

- SPS Owner

3.2.1 Service Developer

The Service Developers write the OSGi service bundles. For the most part, we can consider them to be the Service Provider, however, there are cases where we need to be aware of the distinction. In the case where a Service Developer writes a generally useful bundle and sells it to multiple Service Providers to use in different applications, then there could be complications with code signatures. If, for example, code signatures get used for integrity or for permission assignment, then it could be confusing. If the developer signed the bundle jar files, as we would expect, then any privileges granted based on the signature would be granted based on the developer, not the service provider as is probably desired.

3.2.2 Service Aggregator

A Service Aggregator is a Service Provider that consolidates services provided by other Service Providers into one distinct service, resolving dependencies and conflicts between different services. We think of a Service Aggregator as being somewhat similar to a general contractor that consolidates the services of multiple subcontractors. There is little in this architecture that is specific to a Service Aggregator. Except as noted, everything that is said about a Service Provider also applies to a Service Aggregator.

3.2.3 SPS Manufacturer

The SPS Manufacturer is responsible for integration of the SPS hardware, operating system, virtual machine, and OSGi Framework. Very broadly, there are two cases: (1) the generic SPS, and (2) the special-purpose SPS. The generic SPS would be manufactured to be managed by any SP Operator and to run any bundles, from any Service Provider, as permitted by SP Operator policy. The special-purpose SPS would be manufactured for a specific SP Operator, and a specific type of application bundle. The later case is simpler because keys, certificates, bind address, etc. could be installed at the factory, eliminating the need for a secure protocol to allow these things to be assigned at install time.

3.2.4 SPS Owner

The SPS Owner, as you may guess, owns the Service Platform Server. We mean owner loosely, so it would apply to a lessor, as well. In most cases, we expect the Owner to be a User. However, there are some cases where this may not be true. A landlord may buy and install a single SPS in an apartment building to be shared by the tenants. Each tenant plays some of the role of Owner, except that there are multiple tenants, and they may not trust each other.

4 Security Considerations

Since this RFC do not specify any functionality, but merely introduces definitions to various entities, no specific security considerations are taken here.

All Page Within This Box

5 Examples

5.1 Multiple independent service infrastructures

In this section we describe how different, independent service infrastructures might show up in the same "system". It should be noted that this is just an example of how things might look, and not a template for how things should be done. The scenario is as follows:

A homeowner has a local network onto which the following devices are connected:

- A PC used by the family for various tasks; web surf, e-mail, gaming, etc. An OSGi Service Platform is also running on the PC, since the homeowner subscribes to a news service from news agency N, and this service requires a local service application.
- A washing machine of brand X, The networking capabilities of the machine allows it to be remotely diagnosed. It also supports business models where the homeowner pays for each use of the machine.
- A communication gateway that is able to pass traffic between the local network and Internet. The gateway contains functions to configure and secure the local network. This may include such things as firewall, DHCP server, etc.

The following parties resides outside the home:

- The news agency N, which provide content to the service application running on the PC in the home.
- The washing machine manufacturer.
- The local repair shop that represents X. They will operate services that make remote diagnosis of the washing machine and registers payable events. Both these functions rely on service application(s) presence in the washing machine. This means that the washing machine is also equipped with a Service Platform.
- The Gateway operator, who is takes the responsibility to provide a set of services related to the communication gateway. Some of these services require service applications to be present on the communication gateway, why it is equipped with a Service Platform. The services that the Gateway operator typically provides are; Internet access, network administration of the local network (ensure that the devices on the local network have relevant access both within the local network as well as to/from the Internet). The Gateway operator may also provide a number of other services that are suitable to host on the communication gateway "box".

The following tables show the various entities involved and some typical distribution of roles.

The first table lists the different Service Platform instances:

Service Platform	Service Platform Operator
Inside home PC	Home owner

All Page Within This Box

Inside communication gateway	Gateway operator
Inside washing machine	Local repair shop

The next table lists the different services:

Service	Service Provider	Service User	Service Application in	Service Deployment Manager	Service Operations Support
News	News agency N	Home owner	Home PC	News agency N (or possibly home owner)	News agency N
Internet access	Gateway operator	Home owner	Communication gateway	Gateway operator	Gateway operator
Network management of home network	Gateway operator	Home owner	Communication gateway	Gateway operator	Gateway operator
Washing machine diagnostics	Manufacturer X	Home owner	Washing machine	Local repair shop	Local repair shop
Washing machine pay per use	Manufacturer X	Home owner	Washing machine	Local repair shop	Local repair shop and/or Manufacturer

From the table above we may extract three different service infrastructures that have nothing more in common than that they support the same Service User. No other entities are shared between them.

The figure below shows the three different service infrastructures (one ellipse for each of them). What this picture shows that there are dependencies among the three structures, namely that the leftmost and rightmost ones depends on the communication infrastructure provided by the middle-one.

All Page Within This Box

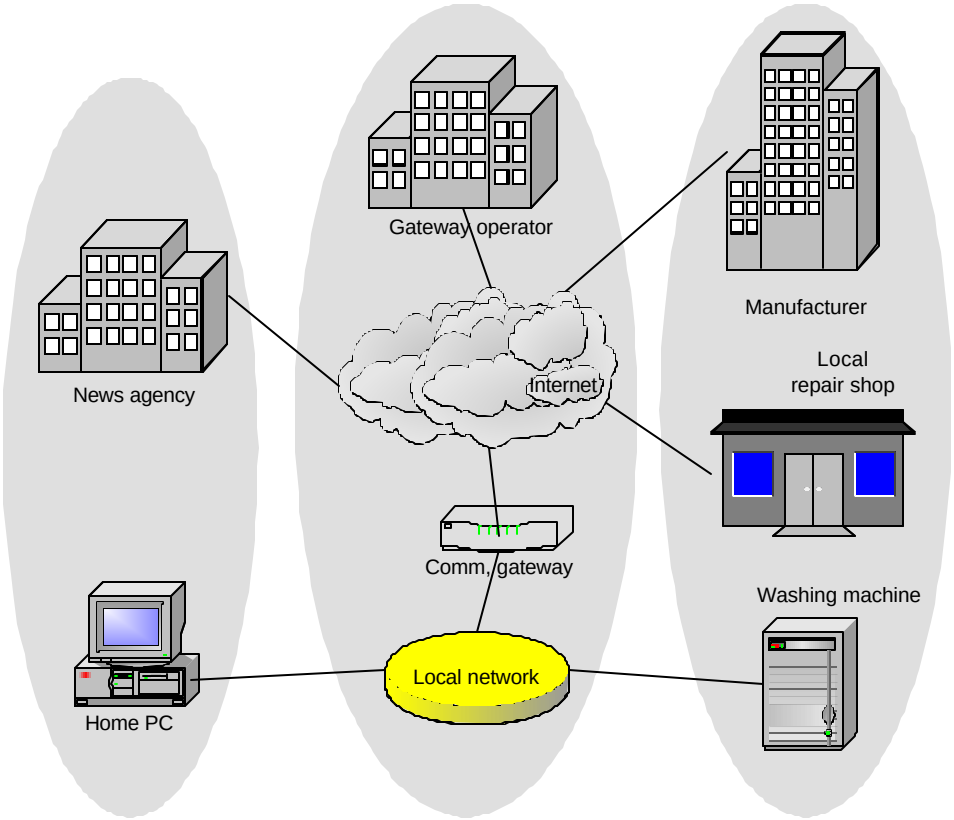

Figure 2: Three independent service infrastructures

All Page Within This Box

5.2 Common service providers

This following sub-sections defines a set of commonly used service providers.

5.2.1 Accounting Provider

The accounting provider performs basically two things in cooperation with the SP. First of all it may grant (or deny), the SP to perform a specific service for a specific Service User and secondly it may store and/or forward charging events coming from the SP.

5.2.2 Certification Authority (CA)

A trusted third-party organization or company that issues *digital certificates* used to create *digital signatures* and *public-private key pairs*. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Typically a CA makes these certificates available in some common database (usually a directory.) CAs must be trusted in order for their certificates to be meaningful. The CA is part of a public key infrastructure (PKI). A very large PKI may also include a RA, or Registration Authority, or even a LRA or Local Registration Authority that does actual physical verification.

5.2.3 Gateway Operator

In case the SP Server represents a communication gateway, the Gateway Operator is someone that normally takes the following roles:

- Service Provider – among the services you might find, managing the gateway WAN connection, managing the local networks. The latter may span from just ensuring that the local devices will have proper connectivity, to controlling all operations related to these devices.
- Service Platform Operator – for the Service Platform(s) in the SP Server.
- Service Deployment Manager – for the Services running on the Service Platform(s) in the SP Server.
- Service Operations Support – for the Services running on the Service Platform(s) in the SP Server.

5.3 System environment for Service Gateway

One important application for the OSGi framework is its use within communication gateways. Due to this we here define a model that describes the environment of such gateways. The model is shown in the following figure and each of the entities in that model is described in this section.

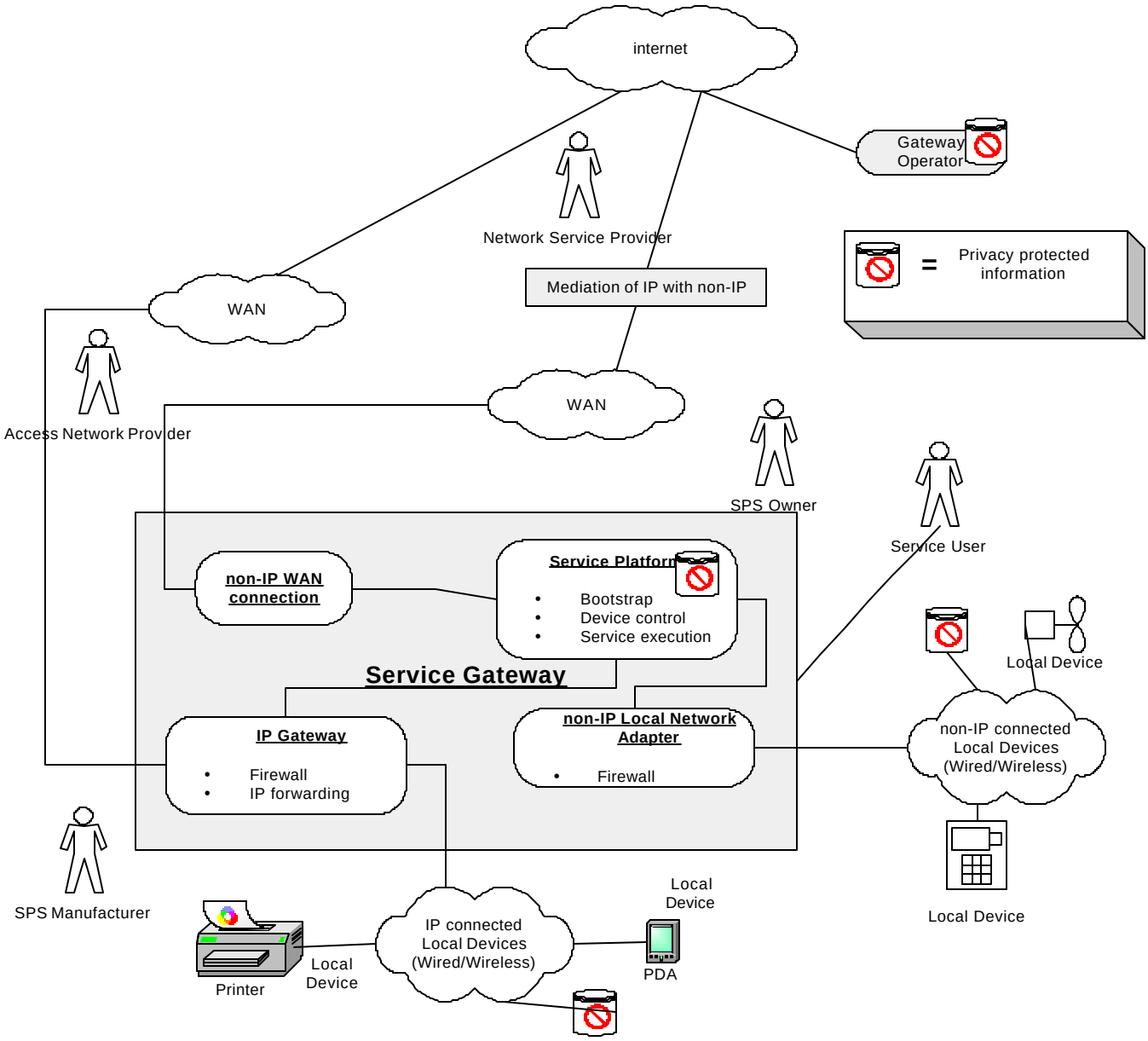

Figure 3: Service Gateway and its environment

All Page Within This Box

5.3.1 Service Gateway

A SP Server is often an IP Gateway, gating between some WAN and one or more local networks. In addition it is also able to execute arbitrary services, and is therefore called a Service Gateway. These separate tasks of a Service Gateway are visible in the model thru the split into a **Service Platform** and an **IP Gateway**. The model also supports Service Gateways with non-IP based WAN connections thru the element called **Non-IP WAN Connection**.

By separating the IP Gateway from the Service Platform it will be “simpler” to apply existing solutions for network- and security management of IP Gateways, to Service Gateways

It should be noted that the split of the Service Gateway is logical and not physical. A typical Service Gateway will probably use a single processor that executes both the Service Platform functions and the IP Gateway functions (and/or Non-IP WAN connection functions).

5.3.1.1 IP Gateway

The IP Gateway deals with forwarding incoming IP traffic, from WAN, LAN, and Service Platform, to their appropriate next hop, WAN, LAN and Service Platform. Firewall functions are typically located in the IP Gateway. The IP Gateway may, from a functional perspective, be viewed as a “standard” access router.

5.3.1.2 Non-IP Local Network Adaptor

Communication with non-IP based local networks, is done thru an adaptor for that specific type of network. This adaptor may include functions such as, firewall, address translation, etc.

5.3.2 WAN

A Service Gateway is typically connected to some kind of Wide Area Network (WAN). Typically a Service Gateway is connected to just one WAN, but multiple WANs connected to a single Service Gateway are not excluded. Typical WAN technologies are:

- DSL
- Ethernet
- Cellular phone networks (e.g. GSM, AMPS)

5.3.2.1 IP WAN

Most commonly the WAN is used to carry IP traffic. A WAN with the capability of carrying IP traffic is called an IP WAN.

5.3.2.2 Non-IP WAN connection

Some Service Gateways will not have IP connectivity, or will just have IP connectivity under special circumstances. For example a Service Gateway in a car may communicate with its Gateway Operator, etc., using some native wireless protocols (e.g. GSM SMS).

5.3.2.3 Mediation of IP with non-IP

Gateway Operators, Service Providers/Aggregators are typically connected to the Service Gateway using Internet. In order for them to communicate with Service Gateways, which are not capable of communicating using IP, some kind of mediation of the communication is required. The purpose of this element is to perform the necessary mediation. A typical example could be a WAP Gateway.

5.3.2.4 Access Network Provider

The Access Network Provider provides and manages the media used to access the Service Gateway from the outside. This would refer to the Data-Link layer in the OSI Reference Model, and probably also the Physical layer. For example, a Service Gateway that connects to the outside using DSL might very well have (in the aftermath of deregulation) five companies responsible for the various layers: the phone company responsible for the copper wires to the home, the DSL service provider responsible for the ATM connectivity, the ISP responsible for Internet connectivity, the Gateway Operator responsible for operation of the Service Gateway, and finally the other Service Provider(s) responsible for the value added service(s) running on the gateway. (The Service Provider is not technically layered on top of the Gateway Operator in the sense that, the data is not encapsulated by the Gateway Operator, but only in the sense that the Service Provider is dependent on the Gateway Operator to keep the gateway functioning)

The Access Network Provider plays a limited role in this architecture. In the example, it is not directly visible to the Service Gateway or the Gateway Operator, rather only indirectly through the Network Service Provider.

5.3.2.5 OSG Network Service Provider

The Network Service Provider provides and manages wide-area network connectivity between the Service Gateway, and outside parties. The outside parties include the Gateway Operator and other Service Providers. In the case where the Service Gateway is connected via Internet, the Network Service Provider would be the Internet Service Provider (ISP).

It is our intent that this architecture applies to both IP and non-IP network layers, and to both continuous and intermittent availability. We make every effort to avoid making assumptions that the Network Service is Internet (IP) or that it is continuously available, however, we may sometimes say *ISP* when we really mean to say *Network Service Provider*.

In an IP network, it is common for the ISP to assign IP addresses, often dynamically using DHCP. This could complicate our approach to authentication and key exchange. Most non-IP networks have a similar issue.

5.3.3 Local buses & local devices

5.3.3.1 Local buses

A local bus is used for communication with local devices. The technologies differ dependent on various factors like

- Type of Service Gateway (e.g. residential, vehicle)
- Market (e.g. US, Europe)

Typical technologies are:

- EIB (European Installation Bus)
- Ethernet
- Wireless Ethernet
- Firewire
- MOST

5.3.3.2 Local Devices

A Local Device is something that is connected to the local buses and that is:

- sending and/or receiving information from the Service Platform

and/or

- sending and/or receiving information thru the IP Gateway

The purpose of this distinction is to separate devices that are able to communicate thru the IP Gateway from devices that must communicate thru the Service Platform. Security solutions for these two cases are somewhat different and therefore this distinction is made.

5.3.3.3 IP Connected Local Devices

Some local devices are connected to the Service Gateway using IP.

5.3.3.4 Non-IP Connected Local Devices

Some local devices are connected to the Service Gateway using other “network” technologies than IP.

5.3.4 Internet

This could be the public Internet or any private network based on IP technology or a combination of both.

5.3.5 Privacy protected information

Information that is vital not to expose to unauthorized parties are held at various places in the total environment. In the model such information is denoted “Privacy protected information”.

6 Document Support

6.1 References

[1]. Bradner, S., Key words for use in RFC’s to Indicate Requirement Levels, RFC2119, March 1997.

6.2 Author’s Address

Name	Lars-Erik Helander
Company	Gatespace AB
Address	Stora Badhusgatan 18-20 SE-411 21 Gothenburg Sweden

All Page Within This Box

Voice	+46 31 743 98 43
e-mail	helander@gatespace.com

6.3 Acronyms and Abbreviations

6.4 End of Document

All Page Within This Box