

# **Operational Manual For SSDG**

# Table of Contents

<b>ABBREVIATIONS</b> .....	<b>5</b>
<b>SECTION 1: INTRODUCTION</b> .....	<b>6</b>
<b>1 INTRODUCTION</b> .....	<b>7</b>
1.1 INTENDED USER.....	7
1.2 HOW TO USE.....	7
1.3 ORGANIZATION OF THE MANUAL.....	8
1.4 HELPDESK.....	8
<b>2 GATEWAY CONCEPTS</b> .....	<b>9</b>
2.1 OVERVIEW.....	9
2.2 SERVICES OFFERED BY SSDG.....	10
2.3 BENEFITS OF SSDG.....	10
2.4 GOVERNMENT DEPARTMENTS.....	11
2.4.1 Service Access Providers.....	11
2.4.2 Citizens.....	12
2.5 GATEWAY COMPONENTS.....	12
2.6 OVERVIEW OF THE GOVERNMENT GATEWAY ARCHITECTURE.....	12
2.7 LEVELS OF AUTHENTICATION.....	16
2.7.1 Authentication with username and password.....	16
2.7.2 Authentication using encryption technique.....	16
2.7.3 Authentication using W3Csignature.....	16
2.8 DEPLOYMENT OF SSDG.....	16
<b>SECTION 2: SP AND SAP</b> .....	<b>17</b>
<b>3 INTEGRATION OF DEPARTMENTS (SERVICE PROVIDER- SP)</b> .....	<b>18</b>
3.1 WHO IS A SERVICE PROVIDER?.....	18
3.2 ROLE OF SP.....	18
3.3 WHAT ARE SERVICES?.....	18
3.4 SYNCHRONOUS AND ASYNCHRONOUS SERVICES.....	18
3.4.1 Asynchronous Services.....	18
3.4.2 Synchronous Services.....	18
3.5 REGISTERING AN SP.....	19
3.5.1 Updating an SP.....	19
3.5.2 De-Registering an SP.....	21
3.6 REGISTERING SERVICES OF SP.....	21
3.6.1 Updating Services of SP.....	22
3.6.2 De-Registering Services of SP.....	23
3.6.3 Connector Development for SP.....	23
3.7 PREREQUISITES – PREREQUISITES FOR CONNECTING SP THROUGH SSDG ALONG WITH TIME LINES	23
3.7.1 Domain Name Registration.....	23
3.7.2 SSL certificate procurement.....	24
3.7.3 Connector.....	25
<b>4 INTEGRATION OF SERVICE ACCESS PROVIDER (SAP)</b> .....	<b>26</b>
4.1 WHO IS A SERVICE ACCESS PROVIDER?.....	26
4.2 ROLE OF SAP.....	26
4.3 CONNECTOR DEVELOPMENT FOR SAP.....	26

4.4	REGISTERING A SAP .....	26
4.4.1	Updating a SAP .....	27
4.4.2	De-Registering a SAP.....	29
4.5	MAPPING OF SAP WITH SERVICES .....	29
4.5.1	De-Register SAP Registered Service.....	30
<b>SECTION 3: MONITORING .....</b>		<b>31</b>
<b>5</b>	<b>MONITORING AND MANAGEMENT .....</b>	<b>32</b>
5.1	MONITORING THE SSDG.....	32
5.2	REPORT GENERATION .....	36
5.2.1	SLA reports .....	36
5.2.2	SAP reports.....	37
5.2.3	SP reports.....	37
5.2.4	SSDG reports .....	37
<b>SECTION 4: OTHER .....</b>		<b>38</b>
<b>6</b>	<b>CONFIGURATION.....</b>	<b>39</b>
6.1	SSDG.....	39
6.2	ALERTS .....	39
6.3	REPORTING TOOLS/DASHBOARD .....	39
<b>7</b>	<b>ADDITIONAL RESOURCES .....</b>	<b>49</b>

## List of Figures

<i>Figure 1 : Communication between Departments without and with SSDG .....</i>	9
<i>Figure 2 : Architecture of SSDG .....</i>	13
<i>Figure 3 : Constellation of Gateways .....</i>	14
<i>Figure 4 : National Services Directory .....</i>	15
<i>Figure 5 : SP Enrolment Form .....</i>	19
<i>Figure 6 : SP Profile Update Form .....</i>	20
<i>Figure 7 : SP Updation Form .....</i>	20
<i>Figure 8 : SP De-Registration Form .....</i>	21
<i>Figure 9 : Service Enrolment Form.....</i>	22
<i>Figure 10 : Service De-registration Form.....</i>	23
<i>Figure 11 : SAP Registration Form.....</i>	27
<i>Figure 12 : SAP Profile Update Form.....</i>	28
<i>Figure 13 : SAP Updation Form .....</i>	28
<i>Figure 14 : SAP De-registration Form.....</i>	29
<i>Figure 15 : SAP Register Service .....</i>	30
<i>Figure 16 : De-Register SAP Registered Service .....</i>	30
<i>Figure 17 : Login Screen .....</i>	32
<i>Figure 18 : Dashboard .....</i>	33
<i>Figure 19 : Availability of Services and Average Load Graph .....</i>	34
<i>Figure 20 :Escalation .....</i>	35
<i>Figure 21 : Inventory of Servers .....</i>	35
<i>Figure 22 : Memory Charts .....</i>	36
<i>Figure 23 : Add New report.....</i>	40
<i>Figure 24 : Report wizard.....</i>	41
<i>Figure 25 : Locate jrxml file.....</i>	42
<i>Figure 26 : Report Wizard.....</i>	43
<i>Figure 27 : Locate Data Source .....</i>	44
<i>Figure 28 : Login Jasper Server .....</i>	45
<i>Figure 29 :Jasper Server Inventory.....</i>	46
<i>Figure 30 :Input Parameter Screen .....</i>	47
<i>Figure 31: Accessed Report.....</i>	48

## Abbreviations

1. **NeGP:** National e-Governance Program.
2. **SSDG:** State e-governance Service Delivery Gateway
3. **SAP:** Service Access Provider
4. **SP:** Service Provider
5. **SLA :** Service Level Agreement
6. **SDC:** State Data Centre
7. **IIS:** Interoperability Interface Specification
8. **IIP:** Interoperability Interface Protocol
9. **IGIS:** Inter Gateway Interconnect Specification
10. **GCSS:** Gateway Common Services Specification
11. **NSD:** National Service Directory

## Section 1: Introduction

# 1 Introduction

The operational manual is designed to be the starting point for the manuals. This also can be considered as an index for the other manual provided by SSDG.

## 1.1 Intended User

The manual is designed for the users such as state officials as well as the people who are going to deploy the SSDG, develop the applications that are to be connected to the SSDG, maintain the SSDG at its site and the develop the connectors to establish the communication between an application and the SSDG.

## 1.2 How to Use

As mentioned earlier this manual provides the information about what to find where. In addition to the roadmap, it also provides the information about the overall SSDG project, its requirements, various procedures, its stake holders, the roles and responsibilities of the stake holders and the support provided by C-DAC for the product. Consider this manual as the basic or starting point for the SSDG project.

This manual provides an index to the other manuals for SSDG. The following other manuals are provided along with SSDG software.

1. **SSDG user manual** – This manual provides the information about the SSDG software, how to get SSDG and latter the patches related to SSDG, installation process of SSDG and working with SSDG. Installation process of various components of SSDG software is also covered in this manual.
2. **Connector development manual** – Two separate manuals for Java and .net are provided for the connector development. The connector development manual also provides information about the types of connectors, the generic connector API, and the properties etc required for the development of the application specific connectors.
3. **Cook-book for connector development** – This manual provides some scenarios and the templates of the application specific connector template for the given scenarios.

## 1.3 Organization of the Manual

This manual is divided into four sections.

1. **Introduction** – This section provides the information about the use of various manuals provided with this software. This sections information about the gateway, its architecture and concept of gateway in NeGP.
2. **Integration with SSDG** - This section of the manual provides the information about integration of Service Access Providers (SAP) and Service Providers (SP) to SSDG. It covers the topics related to the integration such as how to register services, how to communicate with SSDG, how the mapping between SAP and SP service is established.
3. **Monitoring** – This sections covers the details about the SLA's of SSDG software and all the information about the monitoring support for SSDG.
4. **Other**- Remaining information such as configuring reports, alerts, and some supporting documents.

## 1.4 Helpdesk

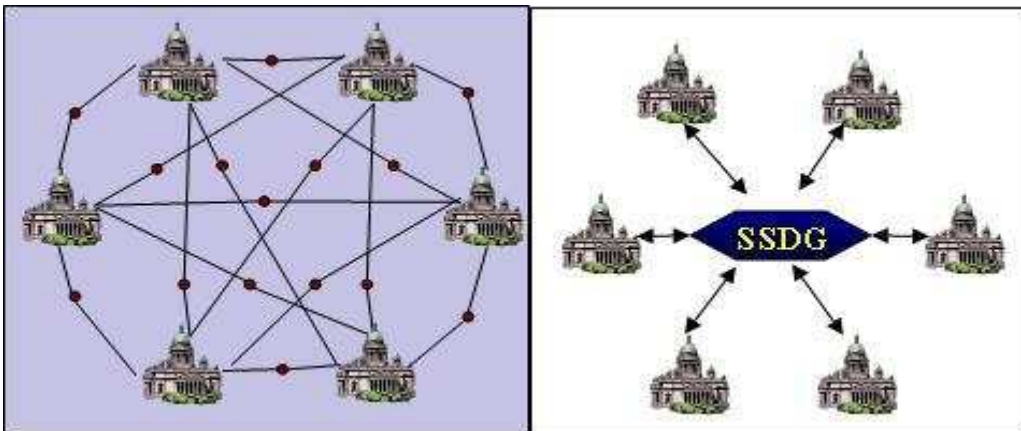
C-DAC provides the helpdesk for the SSDG software product support.

## 2 Gateway Concepts

This chapter covers the information about the gateway project.

### 2.1 Overview

The National e-Governance Plan (NeGP) of the Govt. of India aims to make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realize the basic needs of a common man. One of the goals of the Government to meet this vision is the need to cooperate, collaborate and integrate information across different departments in the Centre, States and Local Government. Government systems characterized by islands of legacy systems using heterogeneous platforms and technologies and spread across diverse geographical locations, in varying state of automation, make this task very challenging. The State e-Governance Service Delivery Gateway (SSDG), a core component in e-Governance infrastructure under the NeGP, can simplify this task by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across.



*Figure 1 : Communication between Departments without and with SSDG*

Figure 1 shows the point to point communication without SSDG as is. This makes it difficult to maintain and upgrade the department applications in the case of version change, change in government policies and business rules. SSDG is an attempt to reduce such point to point connections between departments and provide a standardized interfacing, messaging and routing switch through which various players such as departments, front-end service access providers and back-end service

providers can make their applications and data interoperable. SSDG aims to achieve a high order of interoperability among autonomous and heterogeneous entities of the states based on a framework of e-Governance Standards.

## 2.2 Services Offered by SSDG

SSDG offers the following services.

- Ensures the interoperability among the various departmental applications
- Help protect the legacy investments in software and hardware by easily integrating them with other technology platforms and software implementations.
- De-link the back-end departments/ Service Providers (SP) from the front-end Service Access Providers (SAP) thereby
  - Ensuring separation of concerns of service access from the service implementation i.e. separates the Portal, CSC, Kiosks etc from the government services which reside in the backend departments.
  - Encouraging competition at the front-end by allowing independent service access providers to provide services with varying levels of complexity, cost and service quality levels.
- Reduce the cost of e-Governance Projects by rationalizing, distributing and optimizing the services framework
- Use of PKI infrastructure for secure transactions. Provision exists for encryption of department payload to ensure confidentiality of the department data. SSDG provides digital signature and certificates to all stakeholders interacting with the gateway for identification, authentication and authorization. Transaction and audit logs help track government data.
- Enable transaction logging and time stamping for tracking of transactions and centralized control
- Help the Departments backend workflow evolve gradually as the Gateway acts as a middleware de-linking the backend from the front end. This means that even the Departments which do not have the complete automation or work flow at the back can still deliver e-Service to the citizens in a limited manner through the Gateway.

## 2.3 Benefits of SSDG

SSDG provides benefits to Government departments, Service access providers and citizens.

## 2.4 Government Departments

- **Multiple Delivery Channels:** The position of the Gateway as the middleware will facilitate easy provisioning of government services through various delivery channels seamlessly.
- **Better audit management & time stamping:** Results in better tracking (auditing) and security of each transaction
- **Web enabling of Legacy Applications:** With the use of a Gateway, even legacy applications can be Internet enabled as Gateway server can act as a Web layer around them so government departments need to put least effort for web enabled of their legacy applications.
- **Interoperability:** The gateway positioning as the middleware will facilitate easy inter-departmental data exchange.
- **Seamless availability of information:** The placement of constellation of Gateway Servers at state level will facilitate in getting information and doing transactions by citizens of one state with government department of other states seamlessly.
- **Centralized Management:** The positioning of Gateway Server and building portal of all the departments at a central location, i.e., in State Data Centre (SDC), will help in better centralized Administration, Monitoring, over all maintenance work and deployment of hardware of Web Site at optimal level.
- **Shared Services:** Gateway has the capability to add additional functionality to support shared common services like Authentication, payment gateway interface, etc

### 2.4.1 Service Access Providers

- **Easy interface with departmental data & Business logic:** With the middleware like SSDG in position, the departmental data and business logic reside at the back end and a SAP is in a position to easily integrate with the departmental data and provide value added services.
- **Integrated and joined up services:** With SSDG in position, a SAP could easily provide integrated services to the citizens by fetching data simultaneously from multiple departments or send the service request to one department which could in turn fetch data from other departments and send the same to SAP
- **Modification Flexibility:** With SSDG as the middleware it gives SAP flexibility in modifying the front-end application without touching the back-end applications

## 2.4.2 Citizens

- A citizen can avail the services with providing the minimum data.
- A citizen will get an acknowledgement giving reasonable guarantee that his/her application has reached the destination.
- Citizens will be able to track the status of their request.
- Citizen's data privacy is maintained.
- Grievance can be redressed at one point.
- A citizen will get a single window service catering to multiple departments.

## 2.5 Gateway Components

A gateway consists of two major components: (1) A gateway software product – which consists of messaging engine, a directory service and a management component. The details about these can be found in the *SSDG user manual*.

(2) A software stack: software stack consists of operating system, PostgreSQL database server and JBOSS application server.

SSDG gateway product is developed on the SSDG software stack. Both these software components, a software gateway product as well as the software stack will be provided by C-DAC. The details about the installation of these components can be found in *SSDG user manual*.

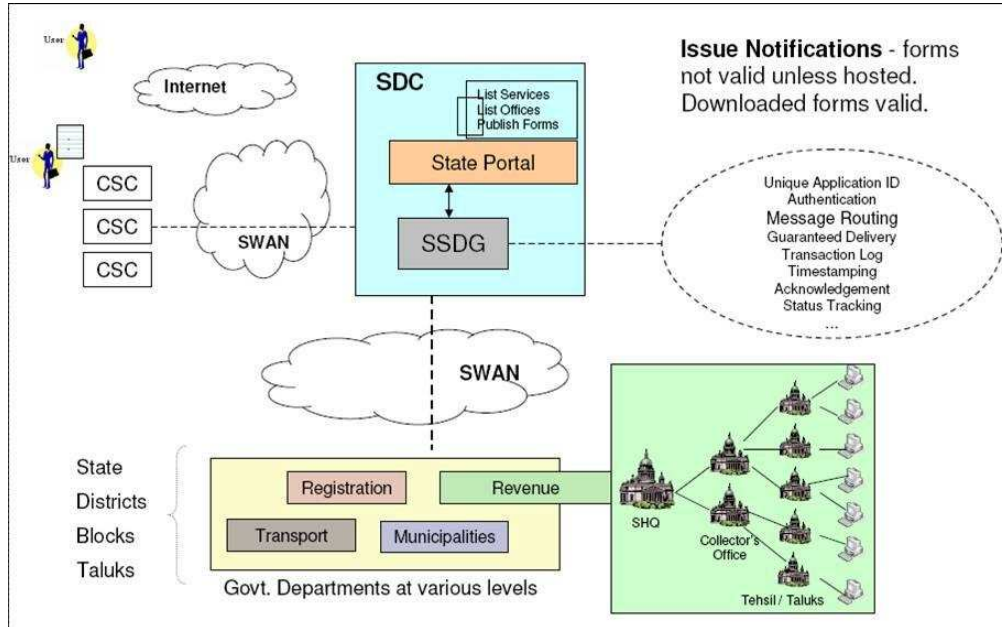
## 2.6 Overview of the Government Gateway Architecture

SSDG as a messaging middleware that acts as an intelligent hub and routes service requests from a Service Seeker (SAP) to a Service Provider (typically a back end Government department that puts up its service for electronic delivery) and in return sends the response back to the Service Seeker through the Gateway.

The gateway achieves integration amongst diverse set of applications built on varying platforms through compliance with a set of e-Governance Specifications- Interoperability Interface Protocol and Interoperability Interface Specifications (IIP/IIS) that are based on open standards such as the W3C XML and SOAP specifications. The Gateway specifications developed for the Gateway messaging and support/common services are

- Interoperability Interface Specification (IIS)
- Interoperability Interface Protocol (IIP)
- Inter Gateway Interconnect Specification (IGIS)
- Gateway Common Services Specification (GCSS)

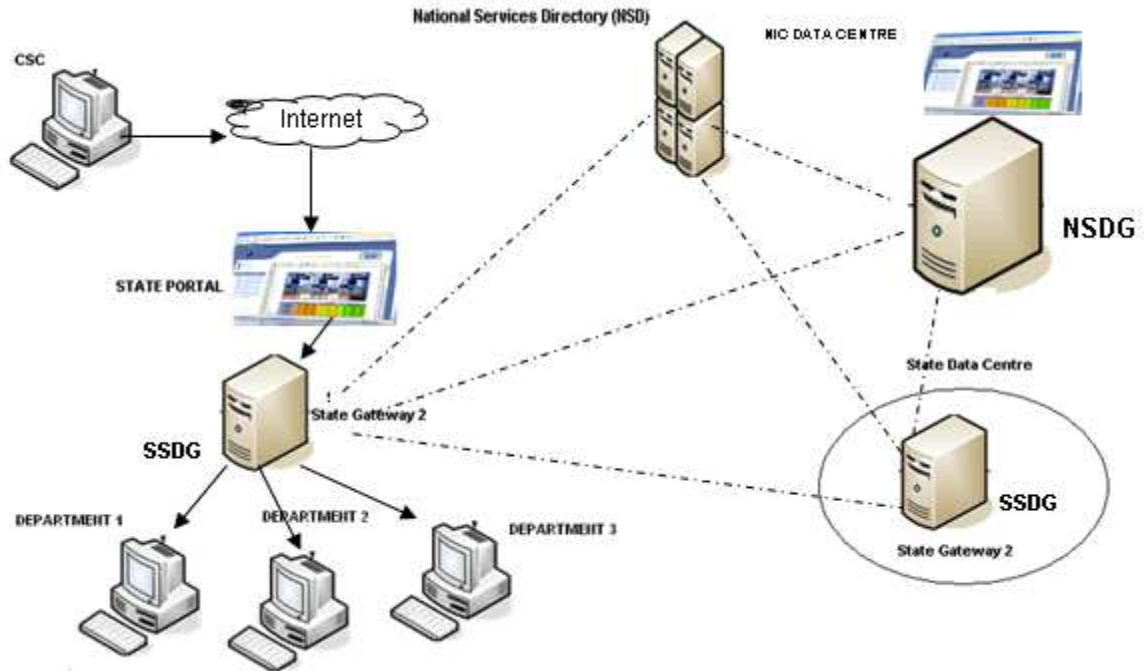
Figure 2 illustrates the SSDG structure linking up the Service Seekers (citizens and businesses), Service Access Providers and the Service Providers (government departments or third party service providers).



**Figure 2 : Architecture of SSDG**

### 2.5.1 Constellation of Gateways

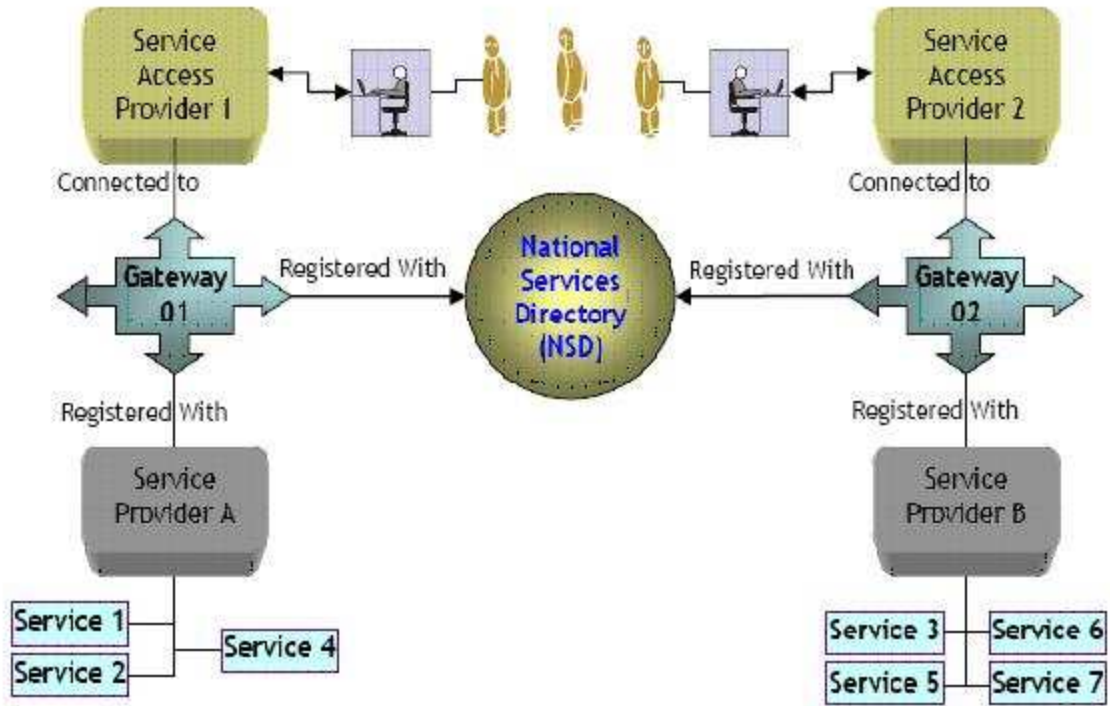
Figure 3 shows the constellation of gateways proposed by DIT. The services offered by SP are registered in National Service Directory (NSD). SAP is allowed to access only the services to which it has permissions. Whenever a requested service is not present at the current gateway level say SSDG, the service is located through NSD. If the SAP has access permissions, SAP is then connected to the appropriate SP offering the desired service. Once the connection is established between the SAP and the desired SP, the information is maintained in the local directory. Constellation of gateway works in this layered manner.



*Figure 3 : Constellation of Gateways*

### 2.5.2 National Services Directory (NSD)

The primary function of the National Services Directory (NSD) is to provide a registry, which acts as a service resolution point for all the services in the Gateway constellation. The Gateways need to register with the NSD before they can attempt to resolve a service from the directory. The services offered by the back-end government departments (Service Providers) will need to be uniquely identified and registered under the administrative domain of the concerned Gateway. During a service life cycle, services may be closed or new services may be added. The Gateway in reality becomes an aggregator of service information within its jurisdiction. Figure 4 shows the working of NSD.



*Figure 4 : National Services Directory*

## 2.7 Levels of Authentication

Every service is registered in SSDG by SP using authentication criteria. The criteria of access control would be decided by the SP as per the requirement of the service provided by back end departments. There are three level of authentication process for availing the services as described below:

### 2.7.1 Authentication with username and password

In this process user would be provided username and password for accessing the service requested. When SAP sends message to SSDG, message includes authentication credential i.e. username & password. Based on user credentials, SSDG will authorize for the access of services.

### 2.7.2 Authentication using encryption technique

In this process user would be provided username and password for accessing the service requested. When SAP sends message to Gateway, credential are included in message after encryption using SHA-1 algorithm. Based on user credential, gateway will decrypt the same and verify the credential for availing service.

### 2.7.3 Authentication using W3Csignature

In this process user would provide digital certificate details i.e. subject-common-name at the time of registration for availing he services. SAP sends message, after signing the appropriate block and placing the signature in the authentication block of message. The signature block also contains certificate in X509 format. Gateway would authenticate using standards of XML Signature implementation process including authentication using subject-common-name for availing the requested service.

## 2.8 Deployment of SSDG

Refer to SSDG User Manual where deployment of both SSDG Product and SSDG Stack is illustrated

## **Section 2: SP and SAP**

## **3 Integration of Departments (Service Provider- SP)**

### **3.1 Who is a service provider?**

The back-end government departments or any other third-party agencies offering e-services to citizens and businesses, and to other government departments, are collectively referred to as Service Providers (SP). Third-party SPs may offer specialized services such as authentication, payment gateway services, or joined-up services.

### **3.2 Role of SP**

SP provides the services to the end users. The services as well as SP need to be registered with the gateway.

### **3.3 What are services?**

Functionality provided by the SP for the citizens are services for example, issuing birth certificate, issuing passport etc.

### **3.4 Synchronous and Asynchronous Services**

SP may provide two types of services

#### **3.4.1 Asynchronous Services**

Services that do not require the connection with the SP fall under the category of Asynchronous service. In this type of a service, SAP requests a service and the gateway sends the acknowledgement back to SAP once the service request is forwarded to SAP. The connection between the SAP and SP need to be present. E.g. putting the request for Birth Certificate.

#### **3.4.2 Synchronous Services**

The services that require the connection between SAP and SP to be present from the point of request to the service gets over. E.g. Getting Unique Id of Citizen.

### 3.5 Registering an SP

The SP should register itself with the gateway in order that its services are accessed by the SAPs. To register, click on the SP Enrolment link. On clicking, a SP enrolment form will appear as below;

**SP Enrolment Form**

<b>Organization Name *</b>	<input type="text"/>
<b>Description *</b>	<input type="text"/>
<b>Contact Person *</b>	<input type="text"/>
<b>Address *</b>	<input type="text"/>
<b>City *</b>	<input type="text"/>
<b>State *</b>	<input type="text" value="STATE"/>
<b>Pin code *</b>	<input type="text"/>
<b>Phone No *</b>	<input type="text"/>
<b>Email Address *</b>	<input type="text"/>

*Figure 5 : SP Enrolment Form*

All necessary information pertaining to the SP is gathered through this registration process. Clicking on the ‘Submit’ button will cause the SP details to be submitted to the gateway. On successful registration, the SP will receive an SP Id through email.

#### 3.5.1 Updating an SP

The SP can update or edit its details by clicking on the ‘SP Profile Update’ link. The link opens a SP Update Profile form as shown below.

**SP Updation Form**

SP ID \*

**Figure 6 : SP Profile Update Form**

The SP is required to submit its SP Id. Once correct SP Id is submitted, a SP Updation form appears. The SP can make desirable changes in the editable fields and submit the form for updation by clicking the 'Submit' button.

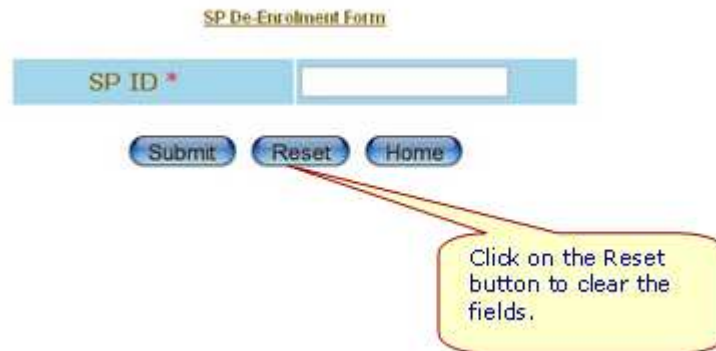
**SP Updation Form**

SP ID *	<input type="text" value="SP0208200840"/>
Organization Name	<input type="text" value="comunitySP"/>
Description	<input type="text" value="comunity sp for registration"/>
Enroll Date *	<input type="text" value="2008-08-02"/>
Contact Person *	<input type="text" value="sanjeev"/>
Address *	<input type="text" value="cdac"/>
City *	<input type="text" value="mumbai"/>
State *	<input type="text" value="ARUNACHAL PRADESH"/>
Pin Code *	<input type="text" value="666666"/>
Phone No *	<input type="text" value="4444444444"/>
Email Address *	<input type="text" value="sanjeevcdac2005@gm"/>

**Figure 7 : SP Updation Form**

### 3.5.2 De-Registering an SP

The SP can de-register itself anytime by clicking on the SP Deletion link. The following screen will appear.



*Figure 8 : SP De-Registration Form*

To de-register from the Gateway, the SP needs to enter its SP ID and click the 'Submit' button. This will de-register the SP from the Gateway. Also, De-registering the SP will automatically de-register all the services pertaining to the SP. (For Service Registration, de-registration, refer section 3.7).

## 3.6 Registering services of SP

The SP needs to register the services it wants to offer on the Gateway. Only by registering these services, the SP can make its services available to the SAP. The services can be registered one at a time by clicking on the 'Service Registration' link. On doing so, the following form will appear;

**Service Enrolment Form**

Service Name *	<input type="text"/>
Service URL *	<input type="text"/>
Description *	<input type="text"/>
Method URL *	<input type="text"/>
Method Name *	<input type="text"/>
Domain *	<input type="text"/>
Authentication Type *	<input type="text" value="-Authentication Type-"/>
Response Type *	<input type="radio"/> Synchronous <input checked="" type="radio"/> Asynchronous
Poll Interval	<input type="text"/>
SP ID *	<input type="text"/>

Click on the Reset button to clear the fields.

**Figure 9 : Service Enrolment Form**

In the above form, the Authentication Type will determine the how the password will be set by the SAP. The Authentication Type may be Messaging Cleartext, SHA1 or Digital Signature.

Also, the Response Type needs to be set for each service which will determine how that service will handle the request coming from a SAP.

On clicking the 'Submit' button, a Service Id will be generated which is automatically registered in the NSD.

### 3.6.1 Updating Services of SP.

The registered services of the SP cannot be updated but can be de-registered and re-registered again with the desired changes. Thus, in order to modify a particular service, the SP needs to first de-register it and then register it again using the Service Registration Form with the desired changes. Services that are registered or de-registered are added and removed both form the Gateway and NSD.

### 3.6.2 De-Registering Services of SP

The services of an SP can be de-registered by clicking the Service De-Registration link. The following form will appear. The SP is required to enter the Service Id of the service it wishes to de-register. Finally, clicking the 'Submit' button will de-register the corresponding service of the SP. It is worthwhile noting here that the de-registered service shall be removed from the Gateway as well the NSD.



*Figure 10 : Service De-registration Form*

### 3.6.3 Connector Development for SP

Refer to the *Connector Development manual in Java and .NET*.

## 3.7 Prerequisites – prerequisites for connecting SP through SSDG along with time lines

### 3.7.1 Domain Name Registration

Normally, a SP will be one of the state government departments. If the SP already has a domain name registered or is using a sub-domain then registration of a new domain name is not required. In case there is no domain name registered or the department wants to provide these services through another domain name then the same can be achieved by following the steps as listed below. As SP is a government department, domain name under GOV.IN domain shall be used.

*Step i:* Go to *registry.gov.in* and check for the eligibility criteria. If your department is eligible then proceed further.

*Step ii:* Click on sign-up link and fill in the details to create a login with the *registry.gov.in*. For each department only one login is required to be created. Multiple domains can be managed through single login. This is an online activity and you will receive registrant-id on e-mail.

*Step iii:* Use the registrant-id as provided on e-mail and login to *registry.gov.in*. Perform *Check Availability* for the proposed domain name. If not available, check for alternate domain name.

*Step iv:* Register the *Domain Name request* using Online Registration service available at *registry.gov.in*.

*Step v:* Submit an Authorization letter in physical format to the address provided on the *registry.gov.in* at the earliest but not later than 30 days of completing the online registration. Otherwise, the request will stand cancelled and the domain name shall be released to others. Format of the letter is provided at *registry.gov.in*.

*Step vi:* The domain name is activated within a week of receiving the authorization letter.

*Step vii:* You also need to provide the address of the Primary and secondary name server online at *registry.gov.in* during registration of domain name or after registration through update facility.

*Step viii:* The status of the registration can be verified online through *registry.gov.in*.

The complete process from online registration to activation of domain name will take around 7-10 days. Depending on the days it takes to receive written authorization letter. At present there is no charge for registration with GOV.IN

### 3.7.2 SSL certificate procurement

**Prerequisites:**

This activity can be performed only after the SP has a domain name or sub-domain name with itself.

A SSL certificate can be procured from any authorized CA. It needs to be verified from the CA that the SSL certificate should be under the trust chain of CCA of India.

The SSL certificate can be procured from NIC. For all government agencies, NIC provides SSL certificate free of cost.

The details of all CA can be found at the website of CCA i.e. [cca.gov.in](http://cca.gov.in).

To procure certificate from NIC goto <https://nicca.nic.in> and follow following steps:

*Step i:* Download the Digital Certificate Request Form from the repository link at the home page

*Step ii:* Select SSL server certificate and appropriate Class which is Class 1 in this case. Kindly verify before filling the form. Fill in other details and post it to NICCA office as mentioned in the form.

*Step iii:* Once the completed form reaches NICCA and is approved you will receive a login-id and password where you are required to upload the CSR (Certificate Signing Request). Details on how to generate the CSR can be found in PKI guidelines.

*Step iv:* After you have generated the CSR login on the nicca site and upload the CSR.

*Step v:* You will receive the signed certificate from the nicca within 2-3 working days. Download the same and store in the Keystore as specified in the PKI guidelines.

The complete process takes around 1-2 weeks depending on time taken for the request form to reach NICCA.

### 3.7.3 Connector

Refer to the *Connector Development manual for Java and .NET and Connector Cookbooks in Java and .Net* for implementing connectors.

## 4 Integration of Service Access Provider (SAP)

### 4.1 Who is a service access provider?

A Service Access Provider is an entity, which facilitates government service access by Service Seekers, by providing a front-end infrastructure. Linked to the Service Access Providers will be the Delivery Channels, which would be the access mechanism for the citizens and businesses to avail the e-governance services.

### 4.2 Role of SAP

SAP provides the access for the end user to avail the services of the SP. The SAP needs to be registered with the gateway.

### 4.3 Connector development for SAP

Kindly refer the *Connector Development Manual in Java and .NET* for SAP Connector Development.

### 4.4 Registering a SAP

The SAP needs to register itself on the Gateway for accessing the services of the SPs. For this, the SAP needs to fill up the necessary details as shown below to register on the Gateway.

All necessary information pertaining to the SAP is gathered through this registration process. Clicking on the 'Submit' button will cause the SAP details to be submitted to the gateway and on successful registration; SAP Id and passwords shall be generated and sent to the SAP through email. This Login ID shall enable the SAP to access services of the SP through the Gateway. Here it is worth noting that there will be 3 passwords generated each of which shall serve a different purpose;

- A regular password for login purpose.

The other 3 passwords are authentication types which serve a different purpose while accessing the services of the SP. They are;

- Messaging cleartext which is the name of the SAP itself.
- SHA1
- Digital Signature.

**SAP Registration Form**

Organization Name *	<input type="text"/>
Description*	<input type="text"/>
Valid Upto	<input type="text"/>
Contact Person *	<input type="text"/>
Address *	<input type="text"/>
City *	<input type="text"/>
State *	--STATE--
Pin code *	<input type="text"/>
Phone No *	<input type="text"/> (WITH STD CODE )
Email Address *	<input type="text"/>

Click on the Reset button to clear the fields.

Terms of Use Disclaimer: Designed, managed and maintained by www.cdacmumbai.in © 011

**Figure 11 : SAP Registration Form**

#### 4.4.1 Updating a SAP

After registering, the SAP can access the services of the SP. The SAP can update or edit its details by clicking on the 'SAP Profile Update' link. The link opens a SAP Update Profile form as shown below.

**SAP Profile Update Form**

SAP ID \*

Click on the Reset button to clear the fields.

**Figure 12 : SAP Profile Update Form**

The SAP is required to submit its SAP Id. Once correct SAP Id is submitted, a SAP Updation form appears. The SAP can make desirable changes in the editable fields and submit the form for updation by clicking the ‘Submit’ button.

**SAP Updation Form**

SAP ID	SAP080920081104
Organization Name	SAP DIGITAL
Description	Digital Signature
valid_Upto	2033-09-28
Contact Person *	kapil kant kmaal
Address *	Powai
City *	Mumbai
State *	RAJASTHAN
Pin Code *	555555
Phone No. *	7777777777
Email Address *	sanjeevcdac2005@gm.

**Figure 13 : SAP Updation Form**

#### 4.4.2 De-Registering a SAP

The SAP can de-register itself anytime by clicking on the SAP De-registration link. The following screen will appear.

**SAP De-registration Form**

<b>SAP ID *</b>	<input type="text"/>
-----------------	----------------------

*Figure 14 : SAP De-registration Form*

To de-register from the Gateway, the SAP needs to enter its SAP ID and click the 'Submit' button. This will de-register the SAP from the Gateway.

#### 4.5 Mapping of SAP with services

The SAP can access the services of the SP by registering to those services. To register to services provided by the SP, click the 'SAP Register Service' link. The following form will appear. Enter the SAP Id and the Service Id of the service that the SAP wishes to register to. Also, enter the date up to which the SAP wants to utilize the respective service. Click the 'Submit' button to confirm the registration.

**SAP Register Service Form**

Service ID *	http://202.141.151.140/31
Sap ID *	SAP080920081104
Valid Upto	10/31/2008

Click on the Reset button to clear the fields.

*Figure 15 : SAP Register Service*

#### 4.5.1 De-Register SAP Registered Service

If the SAP wishes to discontinue use of any particular service, it can do so by de-registering the respective service. To de-register a service, click on the De-Register SAP Registered Service link. The following form will appear;

**De-Register SAP Registered Service Form**

SAP ID *	SAP080920081104
Service ID *	http://202.141.151.140/31

Click on the Reset button to clear the fields.

*Figure 16 : De-Register SAP Registered Service*

Enter the SAP Id and the Service Id to de-register the service. Click on the 'Submit' button to confirm the de-registration.

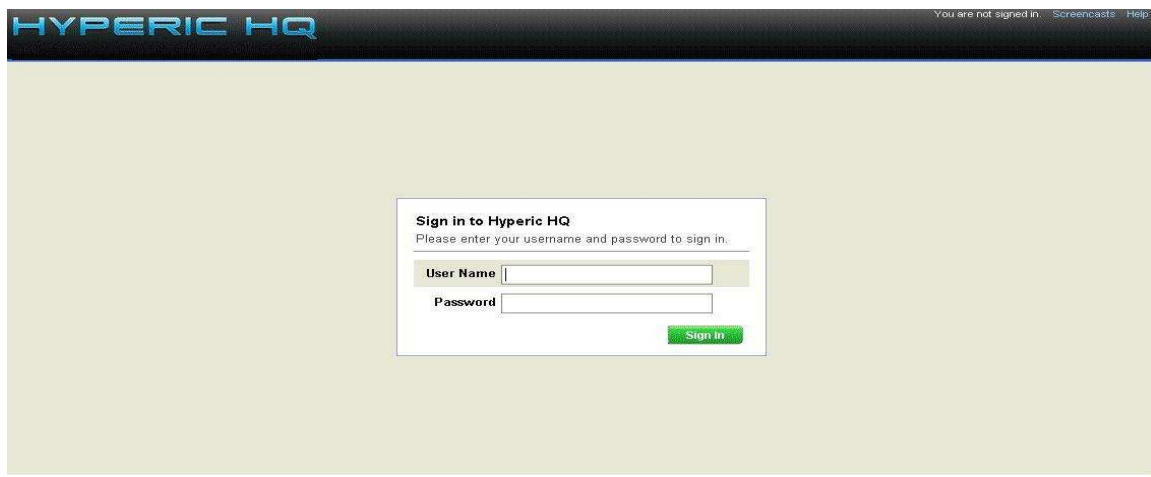
## Section 3: Monitoring

## 5 Monitoring and Management

### 5.1 Monitoring the SSDG

Hyperic HQ monitors every resource of the SSDG infrastructure. It can monitor the health and well-being of operating systems, application servers, web servers, databases, messaging servers and other components of SSDG.

Following are few screen shots showing the monitoring features of Hyperic HQ.



*Figure 17 : Login Screen*

The dashboard features a top navigation bar with the 'HYPERIC HQ' logo, a 'Recent Alerts' notification, and user options like 'Welcome, HQ', 'Sign Out', and 'Screen'. Below the navigation are tabs for 'Dashboard', 'Resources', 'Analyze', and 'Administration'.

The main content area is divided into several sections:

- Search Resources:** A search bar with a 'Resource Name' field and a 'Platforms' dropdown menu.
- Saved Charts:** A section indicating 'No charts to display'.
- Recently Added:** A section indicating 'No resources to display'.
- Availability Summary:** A table with columns for 'Resource Type' and 'Availability', currently showing 'No resources to display, please click the icon above to add resources to portlet.'
- Add content to this column:** A dropdown menu labeled 'Select Portlet'.
- Auto-Discovery:** A table listing discovered resources:
 

Resource Name	Status	Changes
cdac_nsd_msg2.nsdg.gov.in - Red Hat Enterprise Linux 5	modified	server set cl
Tomcat 6.0	new	N/A
JBoss 4.3 default	new	N/A

 Below the table are buttons for 'Add to Inventory' and 'Skip Checked Resources'.
- Favorite Resources:** A table with columns for 'Resource Name', 'Resource Type', and 'Availability', currently showing 'No resources to display, please click the icon above to add resources to portlet.'
- Recent Alerts:** A table listing alerts:
 

Date / Time	Alert Name	Resource Name	Fixed	Act
02/10/2010 11:55 AM	MEMORY_USAGE_GT_90%	cdac_nsd_web2.nsd...	No	

 Below the table are buttons for 'FIXED' and 'ACKNOWLEDGE'.
- Control Actions:** A section with sub-sections for 'Recent Control Actions' and 'Quick Control Frequency', both indicating 'No resources to display'.
- Add content to this column:** A second dropdown menu labeled 'Select Portlet'.

Figure 18 : Dashboard



Figure 19 : Availability of Services and Average Load Graph

**Escalation Name:**

Default Escalation DELETE

Monitoring DELETE

An escalation scheme allows you to order alert notifications and actions. It can be applied to one or more alert definitions.

**Step 1 - Create New Escalation Scheme:**

**Name:**

**Description:**

**If the alert is acknowledged:**

Allow user to pause escalation for

Continue escalation without pausing

**If the alert state has changed:**

Notify previously notified users of the change

Notify entire escalation chain of the change

**If alert is not fixed when escalation ends:**

Stop escalation execution

Repeat escalation actions

Next Step

[<< Return to Administration](#)

*Figure 20 :Escalation*

**Description:** Red Hat Enterprise Linux 5

**Architecture:** x86\_64

**Vendor Version:** Enterprise Linux 5

**Default Gateway:** 10.24.220.1

**Owner:** HQ Administrator (hqadmin) - [Change...](#)

**IP Address:** 10.24.220.14

**OS Version:** 2.6.18-53.el5

**RAM:** 8984 MB

**CPU Speed:** 8 @ 2000 MHz (2x4)

**Vendor:** Red Hat

[Map](#) [Tools Menu](#)

Monitor
Inventory
Alert
Views

**General Properties**

**Description:** Red Hat Enterprise Linux 5 **Date Created:** 08/22/2009 10:36 PM

**Location:** **Date Modified:** 08/22/2009 10:36 PM

**Resource Type:** Linux **Modified By:** HQ Administrator (hqadmin)

[EDIT...](#)

**Type & Network Properties**

**Platform Type:** Linux **Fully Qualified Domain Name:** cdac\_nsd\_msg2.nsdg.gov.in

**Agent Connection:** 10.24.220.14:2144

**IP Address:** 127.0.0.1 **Netmask:** 255.0.0.0

**MAC Address:** 00:00:00:00:00:00

**IP Address:** 10.24.220.14 **Netmask:** 255.255.255.192

**MAC Address:** 00:23:7D:30:67:2A

[EDIT...](#)

**Servers**


**Total Servers:** 4

**Total By Type:** JBoss 4.3 (1)    HQ Agent (1)    Sendmail 8.x (1)

**View:** All Server Types

Server A	Server Type	Install Path	Description	Availability
<input type="checkbox"/> cdac_nsd_msg2.nsdg.gov.in HQ Agent 4.1.2	HQ Agent	/usr/nsdmonitoring/agent/agent-4.2.0	Hyperic HQ monitor Agent	✔
<input type="checkbox"/> cdac_nsd_msg2.nsdg.gov.in JBoss 4.3 production	JBoss 4.3	/usr/nsdmessaging/jboss-eap-4.3/jboss-as/server/production		✔
<input type="checkbox"/> cdac_nsd_msg2.nsdg.gov.in Sendmail 8.x	Sendmail 8.x	/usr/sbin/sendmail		✔

*Figure 21 : Inventory of Servers*



35



Figure 22 : Memory Charts

## 5.2 Report Generation

The Reporting component of SSDG will facilitate various reports for MIS including reports on SLA compliance. SLA Reports with monitoring statistics will be provided on monthly basis.

Following is the list of initial MIS reports for SSDG

### 5.2.1 SLA reports

- Gateway Service Utilization
- Gateway Transaction Performance

### **5.2.2 SAP reports**

- SAP De-registration
- SAP Registration
- SAP Service De-registration
- SAP Service Registration
- SAP Service Utilization

### **5.2.3 SP reports**

- SP De-enrollment
- SP Enrollment
- SP Service De-enrollment
- SP Service Enrollment
- SP Service Utilization

### **5.2.4 SSDG reports**

- List of Gateway Services

## Section 4: Other

## 6 Configuration

### 6.1 SSDG

Refer to SSDG User Manual Section 3.3.4 Installation of Monitoring Component

### 6.2 Alerts

Following is the list of initial email alerts for SSDG –

- Memory Usage
- CPU Usage
- CPU Throughput
- Hard Disc Usage
- Application Server Availability
- JVM Free Memory
- JVM Total Memory
- Database Availability
- SSDG Transaction Response Time

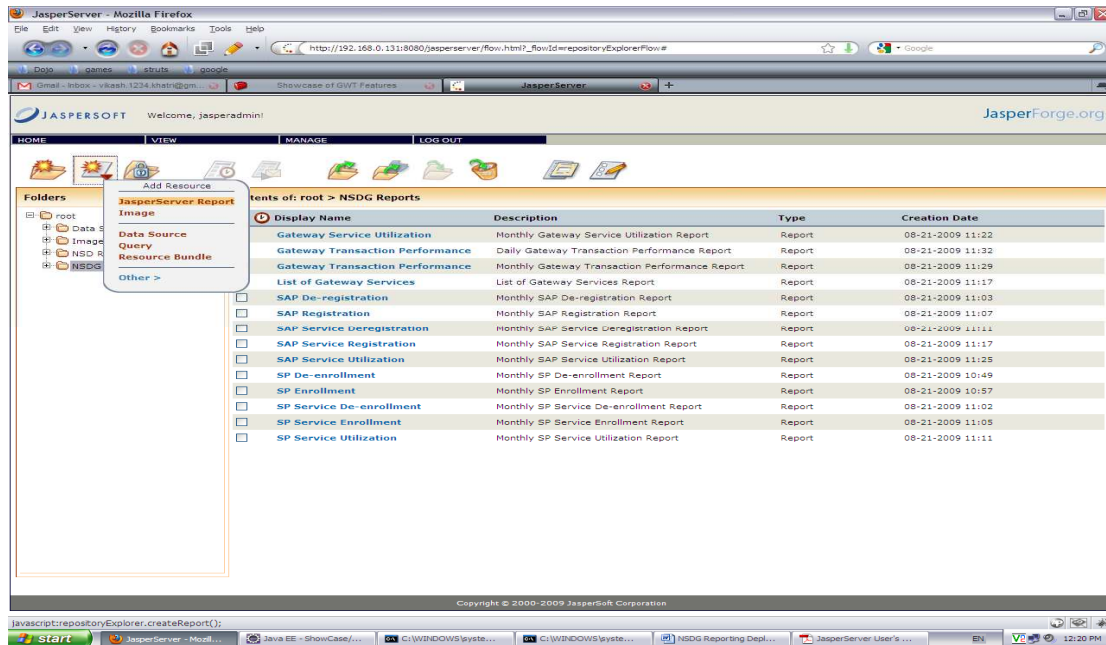
### 6.3 Reporting Tools/Dashboard

Following table describes the tools used in for SSDG reporting subsystem.

<b>Tool</b>	<b>Description</b>
Jasper Server	Open source report server, high-performance reporting management solution
Jasper Reports	Open source reporting engine/API
Jasper iReport	IDE for designing reports

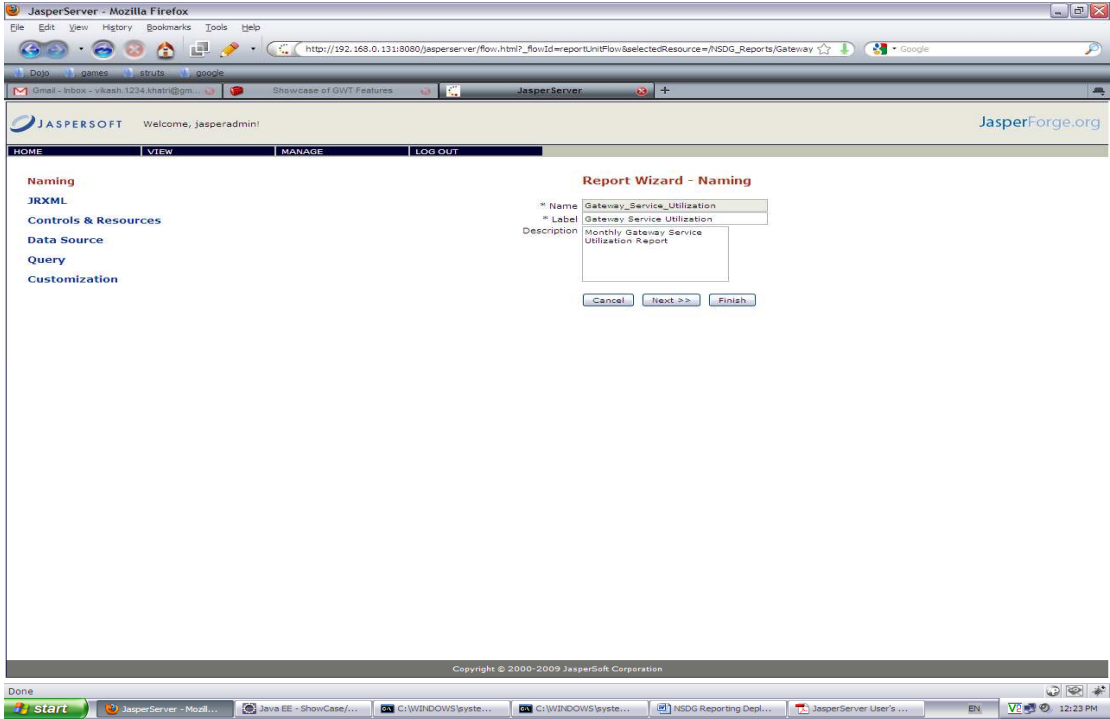
## Adding a new report

1. Select the folder where you want to create a report and select JasperServer Reports option from 'Add Resource' menu.



*Figure 23 : Add New report*

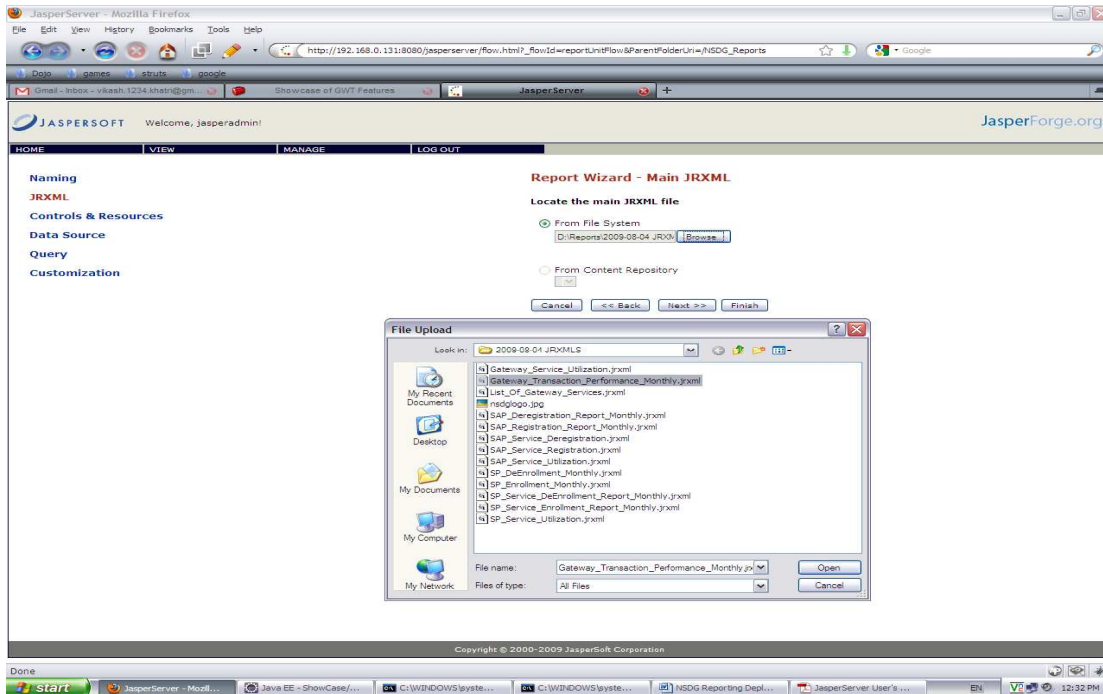
2. The 'Create Report wizard' appears. Enter Name, Label and Description of the report.



*Figure 24 : Report wizard*

And click next.

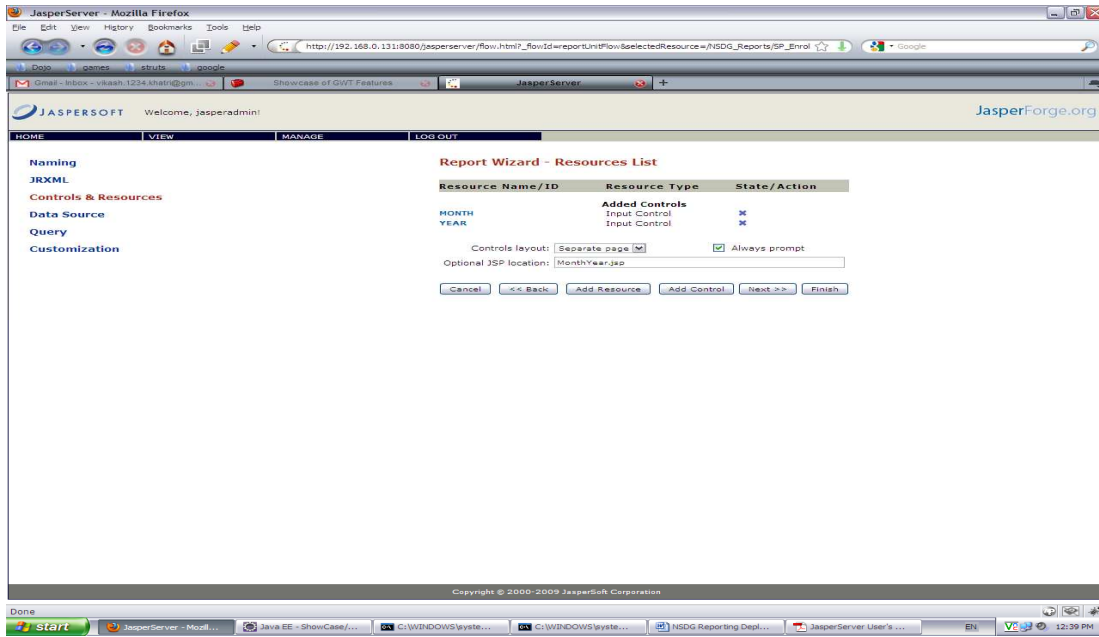
3. Under 'Locate main JRXML File' select the 'From file System' radio button. Click browse button and select the JRXML to be uploaded.



*Figure 25 : Locate jrxml file*

And click next.

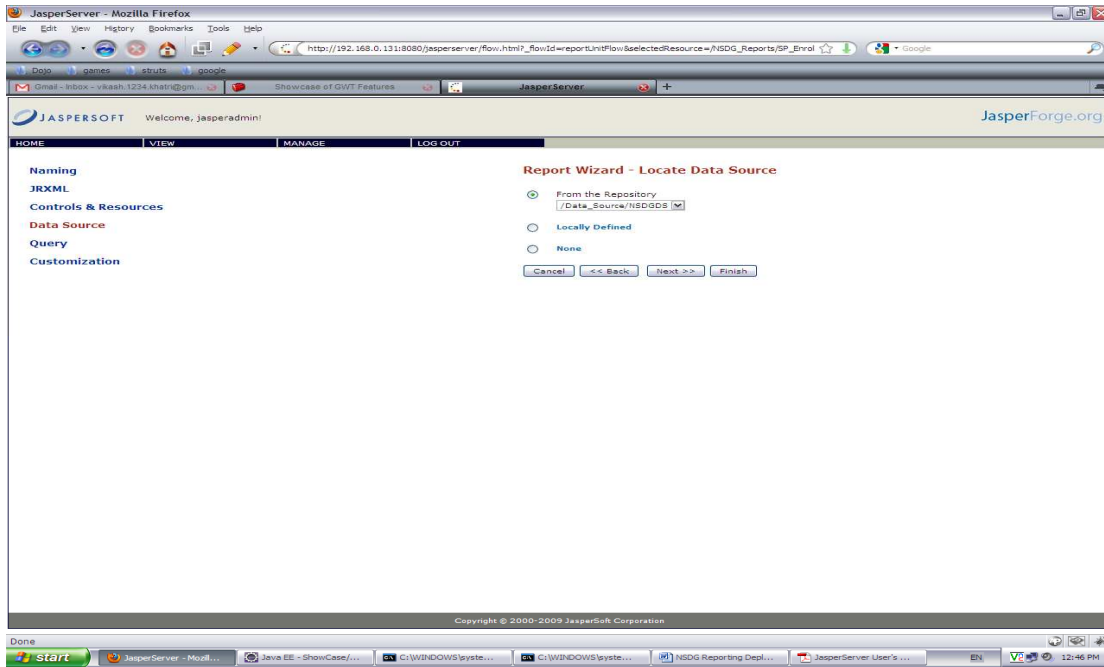
4. Under 'Controls and Resources', you need to add the controls and specify your jsp in 'Optional JSP location'.



*Figure 26 : Report Wizard*

And click next.

5. Under 'Locate Data Source' screen, click on 'From the Repository' radio button and select appropriate data source form combo box.

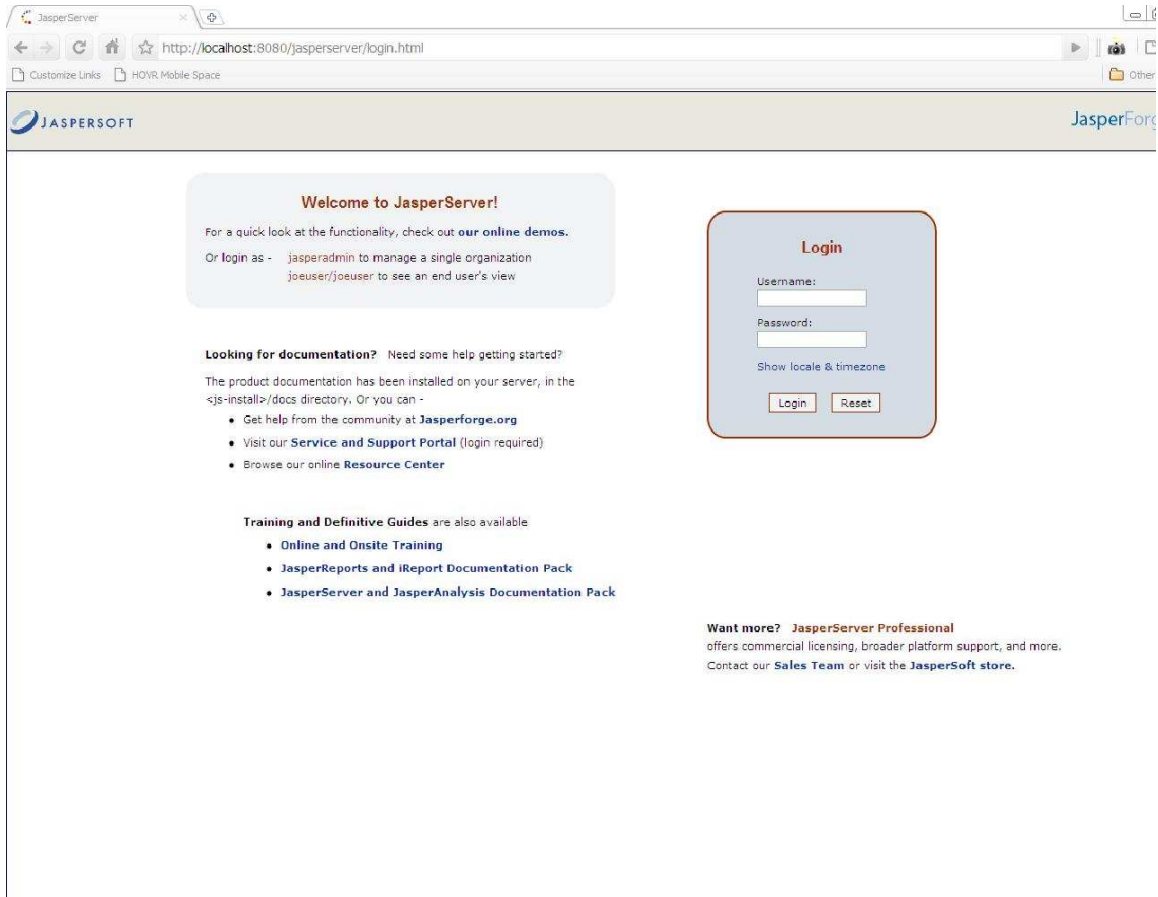


*Figure 27 : Locate Data Source*

6. Click the finish button.

## Japer Server Login Screen

User can login using relevant credentials on Jasper Server login screen. This is the first screen that appears when you access SSDG reporting.



*Figure 28 : Login Jasper Server*

### Jasper Server Report Inventory (Dashboard)

On clicking on “Report” folder user can access Report Inventory with a list of all reports. User can click on a particular report to access it.

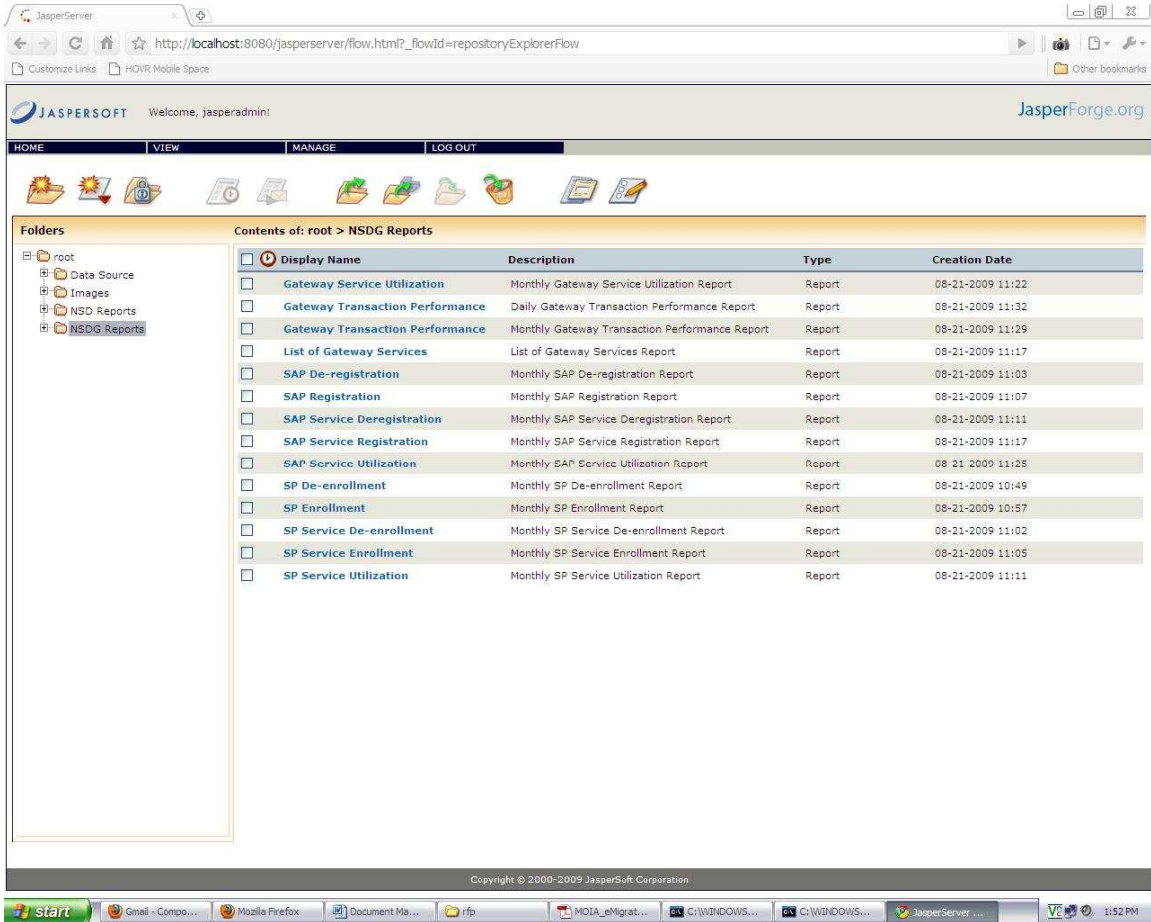
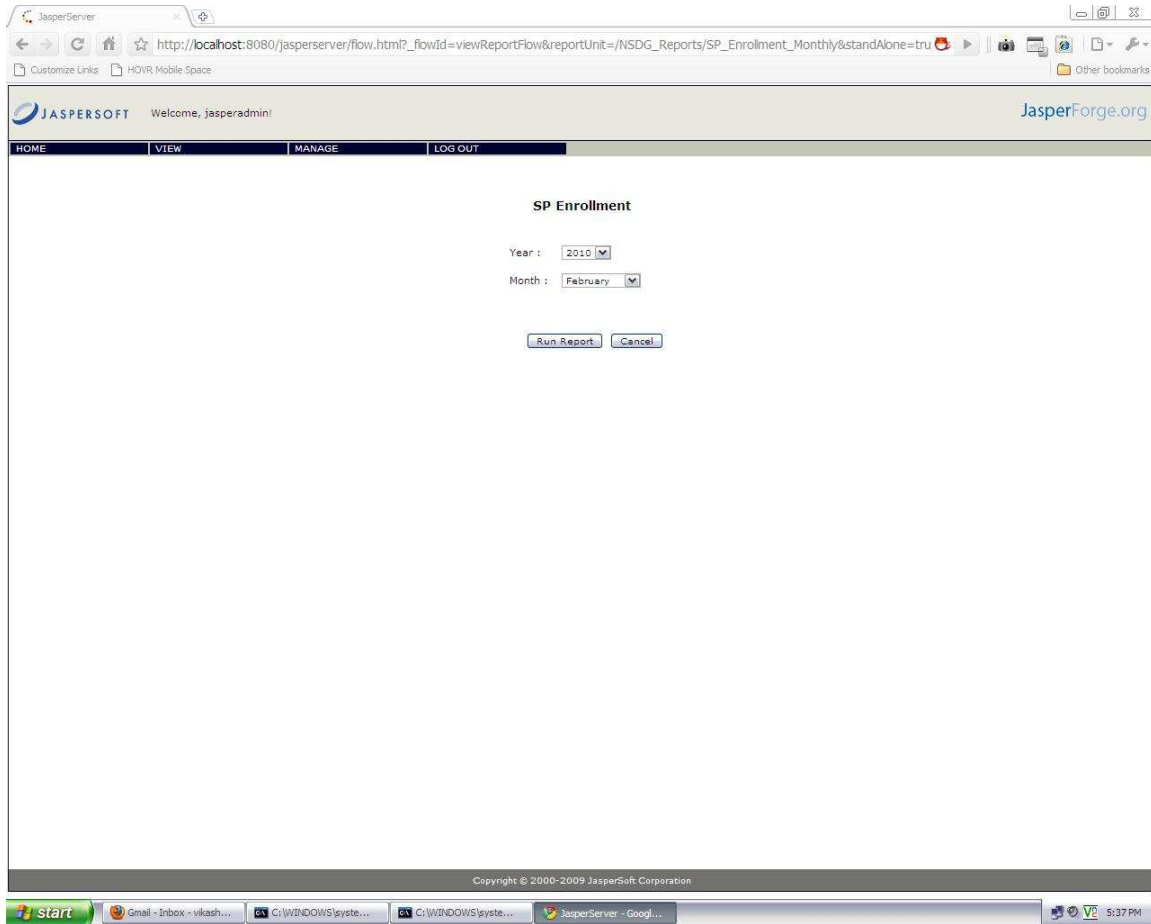


Figure 29 :Jasper Server Inventory

## Input Parameter Screen

Input Parameter Screen appears when a user clicks on a particular screen and the report requires some parameter from the user like period etc. User can input the all fields and click on the “Run Report” button to access the report.



*Figure 30 :Input Parameter Screen*

Once user clicks on “Run Report” button after providing input parameters if any, relevant report will be displayed.

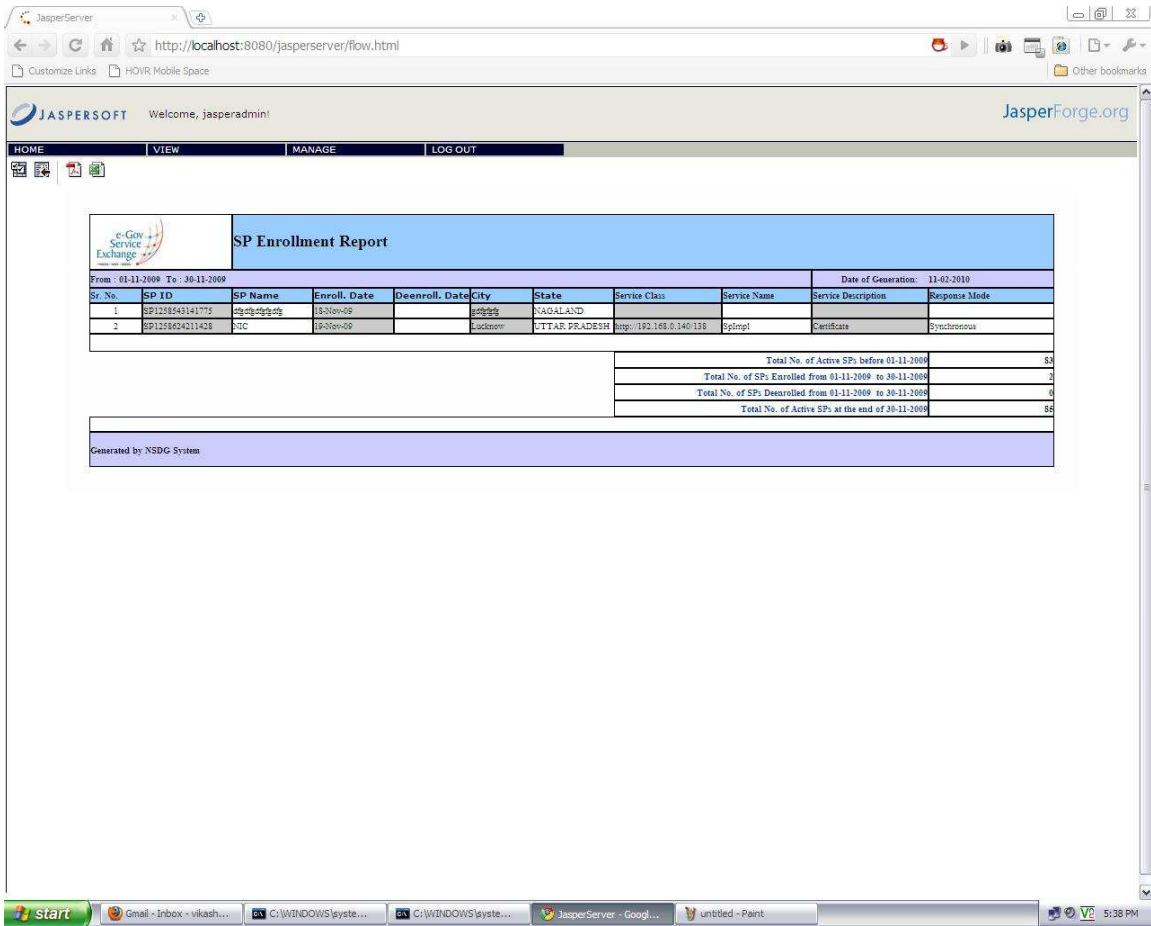


Figure 31: Accessed Report

## 7 Additional Resources

There's more information about operating, deploying and testing SSDG product and SSDG stack. The following list describes where to get more information about other entities like SAP, SP and Connectors related to SSDG software

<i>To know about</i>	<i>Refer</i>
Installation of SSDG Product	SSDG Installation Manual
Installation of SSDG Stack	SSDG Installation Manual
Installation of Operating System	CentOS Installation Manual
Connector Development in Java	Java Connector Development Manual
Connector Development in .NET	.Net Connector Development Manual
PKI features in SSDG	SSDG_PKI Manual
How to register SAP and SP with SSDG	SSDG_Website_Manual
Case study for developing Connectors in Java	Java Connector Cookbook
Case study for developing Connectors in .NET	.NET Connector Cookbook
Troubleshooting and Testing while installing and operating SSDG	Troubleshooting and Testing section of SSDG Installation Manual