Integration Document

for

e-Pramaan: A National e-Authentication Service

Beta V-1.3

Submitted to

Department of Electronics & Information Technology
Ministry of Communications and Information Technology
Government of India

Submitted by

Centre for Development of Advanced Computing

Gulmohar Cross Road No. 9, Juhu, Mumbai 400 049.
Telephone: +91 22 2620 1606, +91 22 2620 1574,
Fax: +91 22 2621 0139, +91 22 2623 2195
Website: www.cdac.in

Table of Contents

1. Revision History

Version	Date	Author	Reason for Change
1.0 (beta)	02-11-14	C-DAC	
1.1 (beta)	22-02-15	C-DAC	Updated the sso-connector.jar and configuration files
1.2 (beta)	25-02-15	C-DAC	Reviewed by AD
1.3 (beta)	19-03-15	C-DAC	Reviewed by Cini

2. Purpose of the Document

The Integration Document details the steps involved in integrating SP services with e-Pramaan. The document provides a step by step instructional guidance to SP application developers in integrating the e-Pramaan including Single Sign-On (SSO) and Single Logout (SLO) aspect facilitated by e-Pramaan. It eventually facilitates the SP's enlistment on e-Pramaan.

3. Intended Audience

The intended audience for this document includes SP Application Developers and the integration agencies as designated by the SPs. The audience is expected to have basic knowledge of Cryptography, Information Security Principles, e-Authentication, Security Protocols as well as Application specific technical expertise (such as Java,.NET,PHP, etc), Web-based Application Design and Development.

4. Comments and Suggestions

For comments, suggestions and feedback on this document, kindly email to epramaan@cdac.in.

5. Document Overview

This document is organized as follows:

- Chapter 1, Project Overview - This section provides an overview of the project objectives.
- Chapter 2, Assumptions - This section covers the assumptions made while integrating SP services with e-Pramaan.
- Chapter 3, Purpose and Scope - This section lays out the overall scope and purpose of e-Pramaan.
- Chapter 4, SP Service Integration with e-Pramaan – This chapter details the integration process to be followed for integrating the SP service with e-Pramaan.

6. Abbreviations

Sr. #	Abbreviation	Full Form
1.	**API**	Application Programming Interface
2.	**ASA**	Authentication Service Agency
3.	**AUA**	Authentication User Agency
4.	**C-DAC**	Centre for Development of Advanced Computing
5.	**DC**	Data Center
6.	**DeitY**	Department of Electronics and Information Technology
7.	**DR**	Disaster Recovery
8.	**MSDG**	Mobile e-Governance Service Delivery Gateway
9.	**NSDG**	National e-Governance Service Delivery Gateway
10.	**SP**	Service Providers
11.	**SSDG**	State e- Governance Service Delivery Gateway
12.	**SSO**	Single Sign On

13.	**TLS**	Transport Layer Security
14.	**SLO**	Single Logout
15.	**AES**	Advanced Encryption Standards
16.	**REST**	Representational State Transfer

7. Standards & Conventions

✓ NSI/IEEE for Integration document Format

8. References

✓ e-Pramaan Standards and Specification Document version 1.2

9. Project Overview

e-Pramaan is a national e-Authentication framework implemented by C-DAC Mumbai for Department of Electronics and Information Technology (DeitY), Government of India. It is a comprehensive framework to authenticate users of various government services in a safe and secured manner for accessing services through both desktop and mobile platforms. e-Pramaan will provide Single Sign On (SSO) and transaction auditing for existing as well as for new users of various government services.

e-Pramaan leverages on Mobile Service Delivery Gateway (MSDG), Aadhaar based Authentication and numerous others to bring uniformity across various authentication mechanisms currently in use by Govt. departments.

10. Pre-requisites

10.1 Assumptions

- Department should communicate with C-DAC or register itself on e-Pramaan department portal.
- Department should have identified an online service to be integrated with e-Pramaan. The service should be production ready to be integrated with e-Pramaan.
- If service chooses Aadhaar based user mapping then Aadhaar Number should be already seeded into the SP side application.

11. e-Pramaan Purpose and Scope

e-Pramaan will provide an added layer of security along with a strong authentication mechanism for users and various government departments availing authentication services at various levels. Users and departments interested in availing the services of the e-Authentication framework should initially register themselves on e-Pramaan. Registration process for SPs is described in detail in the subsequent sections of this document. As a part of the framework, various government departments will be able to integrate with this authentication framework through offered Application Programming Interfaces (API)/ Web Service Interfaces in a smooth and convenient manner without affecting the existing architecture of the running applications.

11.1 Authentication Factors

Authentication is a process in which a user's identity is verified based on the credentials provided by the user during registration or later when (s)he modifies the profile or updates the credentials, such as a password where the assurance mechanism makes sure that "I am who I claim to be". e-Pramaan will provide various levels of authentication in the form of single or multi factor. The factors can be chosen by the departmental services on the basis of sensitivity requirements of the service. Users of e-Gov services, integrated with e-Pramaan will be termed as *SP (Service Provider) users*.

The choice of factor(s) for authentication will depend on the requirements as deemed fit by SPs. Use of additional factors will provide higher level of assurance for a safe and secure e-service experience. Multi factor is stronger than two factor which is stronger than a single factor. Government departments have an option of choosing any one or a combination of factors along with Username as per the combinations described below:

1. **Single Factor** - Any one of the following factors: Password/Digital Signature Certificate (DSC)/Biometrics.
2. **Two Factor**- Combination of any two of the following factors with the chosen single factor: Password/One Time Password (OTP) /Digital Signature Certificate (DSC)/Biometrics.

3. **Multi Factor**- Combination of any two and more of the following factors along with the chosen single factor: Password/ Digital Signature Certificate (DSC) /One Time Password (OTP) / Biometrics.

e-Pramaan shall also provide mobile based authentication mechanism for level 1, 2 and 3, apart from the standard PC based access. For level 3 authentication requiring digital certificates, the use of Proxy SIM/ Crypto SIM Card / External SD Card/Software based certificates shall be considered.

Note: In the current release password and various kind of OTP will be available for services.

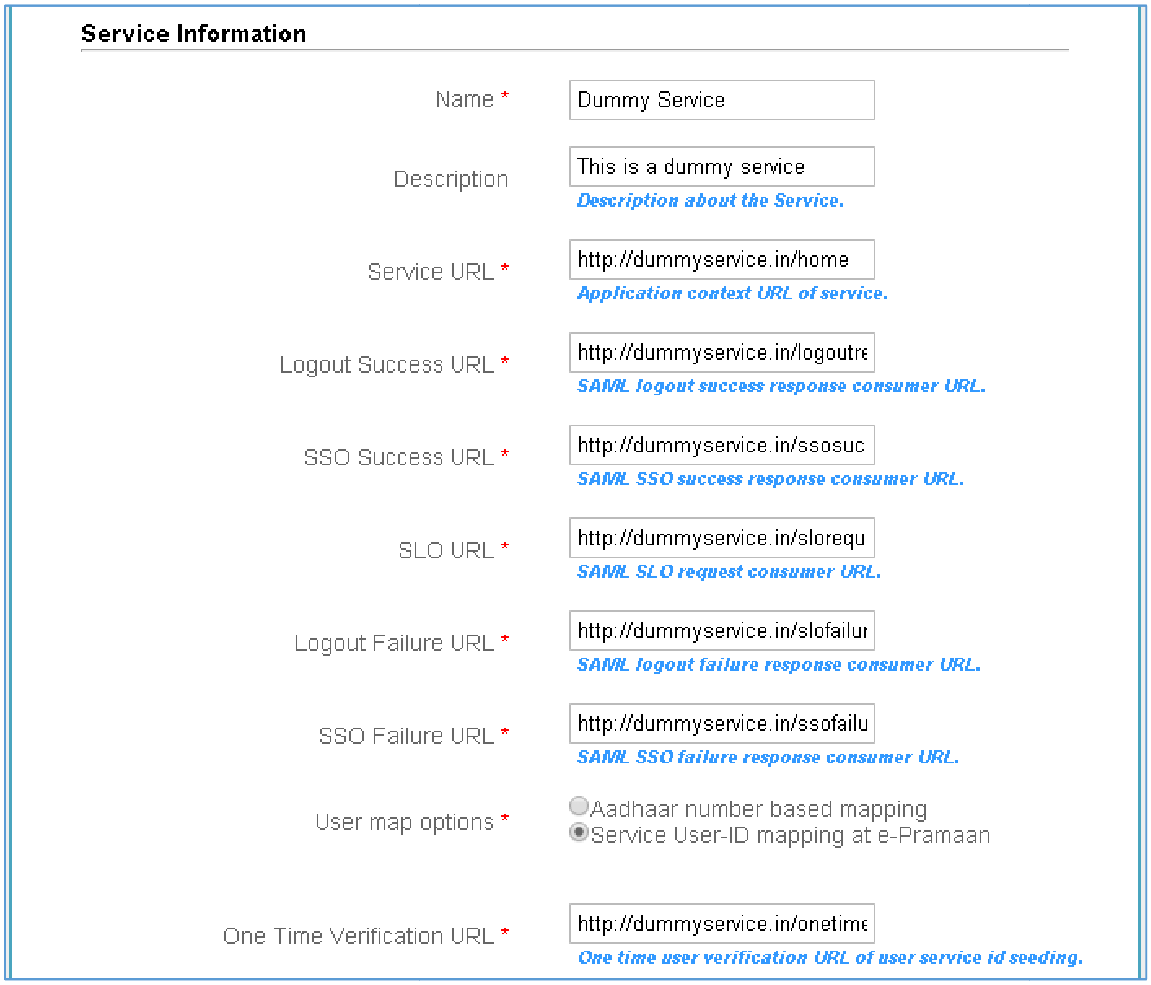
12. SP Service Integration with e-Pramaan

12.1 Service Registration

All SPs which needs to use the authentication service of e-Pramaan, must register with e-Pramaan for the service. This can be done online through the portal sp.epramaan.in. The SP will create a new account at *sp.epramaan.in* and get it activated by the e-Pramaan administrator. After activation, SP can login and register the services which use e-Pramaan for authentication.

Sample screens of service registration by SP are given below.

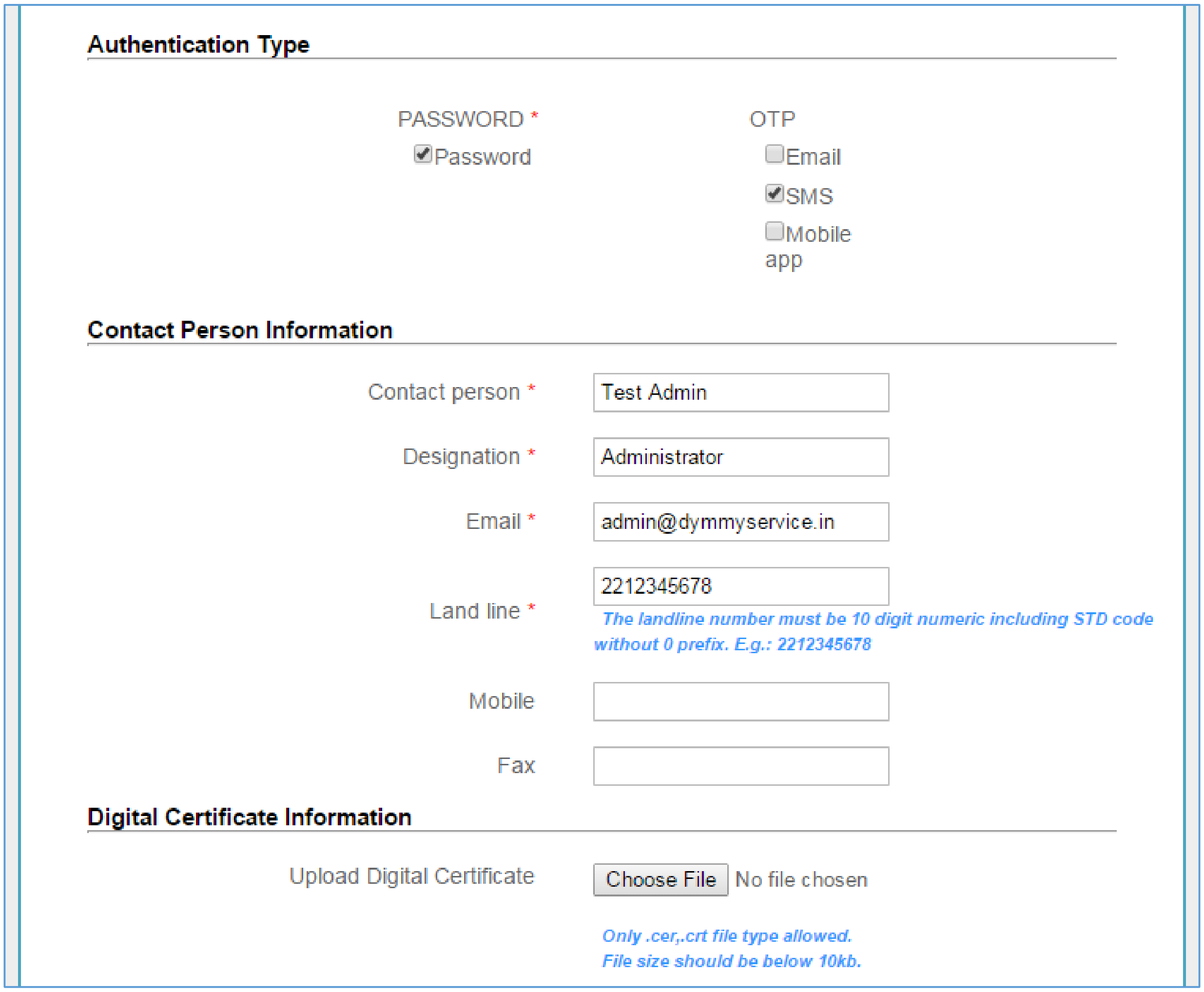
Please note that service will have to register with dummy values, and actual URLs have to be updated according to SP SAML integration.



Service Information

Name *	Dummy Service
Description	This is a dummy service *Description about the Service.*
Service URL *	http://dummyservice.in/home *Application context URL of service.*
Logout Success URL *	http://dummyservice.in/logoutre *SAML logout success response consumer URL.*
SSO Success URL *	http://dummyservice.in/ssosuc *SAML SSO success response consumer URL.*
SLO URL *	http://dummyservice.in/slorequ *SAML SLO request consumer URL.*
Logout Failure URL *	http://dummyservice.in/slofailur *SAML logout failure response consumer URL.*
SSO Failure URL *	http://dummyservice.in/ssofailu *SAML SSO failure response consumer URL.*
User map options *	○ Aadhaar number based mapping ● Service User-ID mapping at e-Pramaan
One Time Verification URL *	http://dummyservice.in/onetime *One time user verification URL of user service id seeding.*

Figure 1 : Adding a Service(1/2)



Authentication Type

PASSWORD *
☑Password

OTP
☐Email
☑SMS
☐Mobile app

Contact Person Information

Contact person *	Test Admin
Designation *	Administrator
Email *	admin@dymmyservice.in
Land line *	2212345678 *The landline number must be 10 digit numeric including STD code without 0 prefix. E.g.: 2212345678*
Mobile	
Fax	

Digital Certificate Information

Upload Digital Certificate No file chosen

Only .cer,.crt file type allowed.
File size should be below 10kb.

Figure 2 : Adding a Service(2/2)

12.1.1 Explanation for fields at https://sp.epramaan.in

The table given below explains how the URLs provided at service registration are mapped to configuration file named epramaan-connector.properties

Sr. #	Field name at *sp.epramaan.in*	Value at sp.epramaan.in
1	Service Url	Application Context of SP service application (`http://dummysp.in/localdemo1`)
2	SSO Url	URL at SP Service which consumes successful SAML authentication response sent by e-Pramaan

		(http://dummysp.in/localdemo1/ssoresponseconsumer)
3	Logout Url	URL at SP Service which consumes successful SAML logout response sent by e-Pramaan (http://dummysp.in/localdemo1/logoutresponseconsumer)
4	SLO Url	URL of the REST Web Service at SP Service which consumes SLO request sent by e-Pramaan (http://dummysp.in/localdemo1/ws/saml/SLO)
5	One time verification URL	The one time verification URL must validate the user at SP Service end and push the verification status to e-Pramaan REST WebService to complete the e-Pramaan User –> Service User Id mapping. Eg: (http://dummysp.in/localdemo1/onetimeverificationurl)
6	SSO Failure URL	URL of the REST Web Service at SP Service which consumes SAML authentication failure response sent by e-Pramaan (http://dummysp.in/localdemo1/ssoresponseconsumer)
7	Logout Failure URL	URL of the REST Web Service at SP Service which consumes SAML logout failure response sent by e-Pramaan (http://dummysp.in/localdemo1/logoutresponseconsumer)
8	Digital Certificate (optional)	A digital certificate with private key is required at SP if requests from SP to e-Pramaan need to be signed. This is recommended for enhanced security but optional. Every service may upload separate digital certificates or use the SP's certificate. Corresponding public certificate for the service must be uploaded https://sp.epramaan.in

12.2 Service application side integration specifics

12.2.1 Mapping of registered values at sp.epramaan.in with epramaan-connector.properties file

The only configuration file for SP Service integration with e-Pramaan is the epramaan-connector.properties file. The config file entries and corresponding values are

Sr. #	Parameter in epramaanconnector.properties	Expected Value	Explanation
1*	ePramaanURL	`https://up.epramaan.in`	e-Pramaan specific (constant value)
2*	SingleLogoutServiceURL	`/processSLORequest.do`	e-Pramaan specific (constant value)
3*	SingleSignOnServiceURL	`/processSSORequest.do`	e-Pramaan specific (constant value)
4	Issuer	ServiceId (Numeric value) given to the service by e-Pramaan when the service is registered at `sp.epramaan.in`	Every service registered with e-Pramaan will be given a unique id called ServiceId.
5	SPServiceHomePageURL	This value corresponds to Service URL at sp.epramaan.in	Base URL / Application Context URL of the SP Service Portal. Eg: http:// dummysp.in /localdemo1
6	SPAssertionConsumerServiceURL	E.g: `/ssoresponseconsumer` This value corresponds to SSO URL at sp.epramaan.in used in SAML creation.	Servlet which will receive SSO Response from e-Pramaan. ***Note:*** *This path is considered relative to the SPServiceHomePage*

			URL
7	SPLogoutConsumerURL	/logoutresponseconsumer This value corresponds to Logout URL at sp.epramaan.in used in SAML creation.	Servlet which will receive LogoutResponse from e-Pramaan**.** ***Note:*** *This path is considered relative to the SPServiceHomePage URL*
8	ePramaanCertificatePath	Path to e-Pramaan.cer	Local file path for Public certificate of e-Pramaan portal. This certificate will be given in the integration kit. It is used by the connector for validating incoming SAML messages.
9*	EncryptionSeed	* This value will be shared with you by e-Pramaan	e-Pramaan mandates all request and responses be encrypted using AES 256 bit encryption. This value will be given by e-Pramaan after registration of Service on SP Portal.
10*	EncryptionSalt	*Service ID of the service	Used for AES encryption. Currently this is the same ServiceId of the service. Refer item (4) above.
11	SamlSigning	True	Set this value ‘True’ (Case sensitive) to enable signing of SAML Request. Any

			other value to disable signing.
12	KeystoreFilePath	Local file path of private certificate used for signing SAML messages.	For signing request/responses, SP Service needs digital certificate with private key.
13	keyPassword	private key is protected using this password.	The password for private key.
14	KeystorePassword	Java specific. Keystore in JKS format will be protected by a password.	Keystore in JKS format will be protected by a password. This password is needed for opening the Keystore.
15	SPCertificateAliasName	Java specific. Certificate alias name	This will be given to SP Service by CA at the time of certificate creation. This value will be used for getting the certificate from the keystore.

*marked entries will be shared by e-Pramaan Administrator.

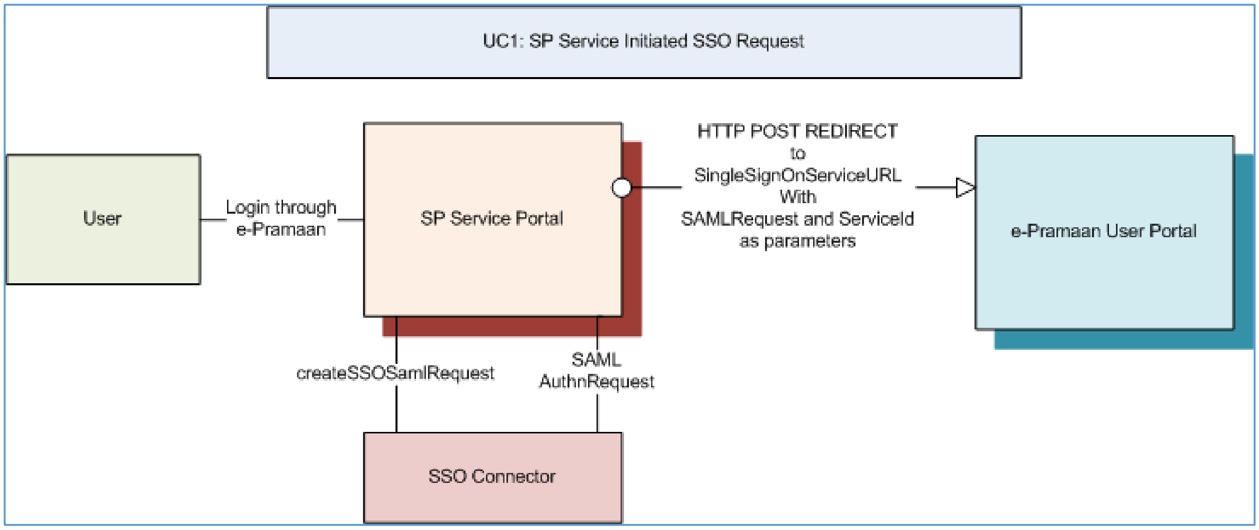
12.2.2 Functionality to be published at SP Service End

Functionality	Purpose	Communication Protocol
SSO Request Creator (12.2.2.1)	When user clicks 'Login using e-Pramaan' Create the SAML request and send to e-Pramaan	HTTP POST
SSO Success Consumer(12.2.2.2)	On authentication, e-Pramaan sends the Service SAML SSO Response. This API	HTTP POST

	consumes the response.	
SSO Failure Consumer(12.2.2.3)	In exception conditions UI control remains on e-Pramaan, a SAML response is sent to Service for audit. This API consumes the response.	RESTful WebService
Logout Request Creator(12.2.2.4)	When user clicks ‘Logout’ Create the SAML Logout request and send to e-Pramaan	HTTP POST
Logout Success Consumer(12.2.2.5)	On logout, e-Pramaan sends Service the SAML Logout Response. This API consumes the response.	HTTP POST
SLO Request Consumer(12.2.2.7)	If the logout is triggered by e-Pramaan, then this API consumes the SAML request to invalidate the Service session	RESTful WebService

12.2.2.1 SSO Request Creator (HTTP POST)

e-Pramaan SAML SSO is initiated by sending SSO request from SP to e-Pramaan. Use case diagram of SSO Request creation is given below.


UC1: SP Service Initiated SSO Request
User
Login through e-Pramaan
SP Service Portal
HTTP POST REDIRECT to SingleSignOnServiceURL With SAMLRequest and ServiceId as parameters
e-Pramaan User Portal
createSSOSamlRequest
SAML AuthnRequest
SSO Connector

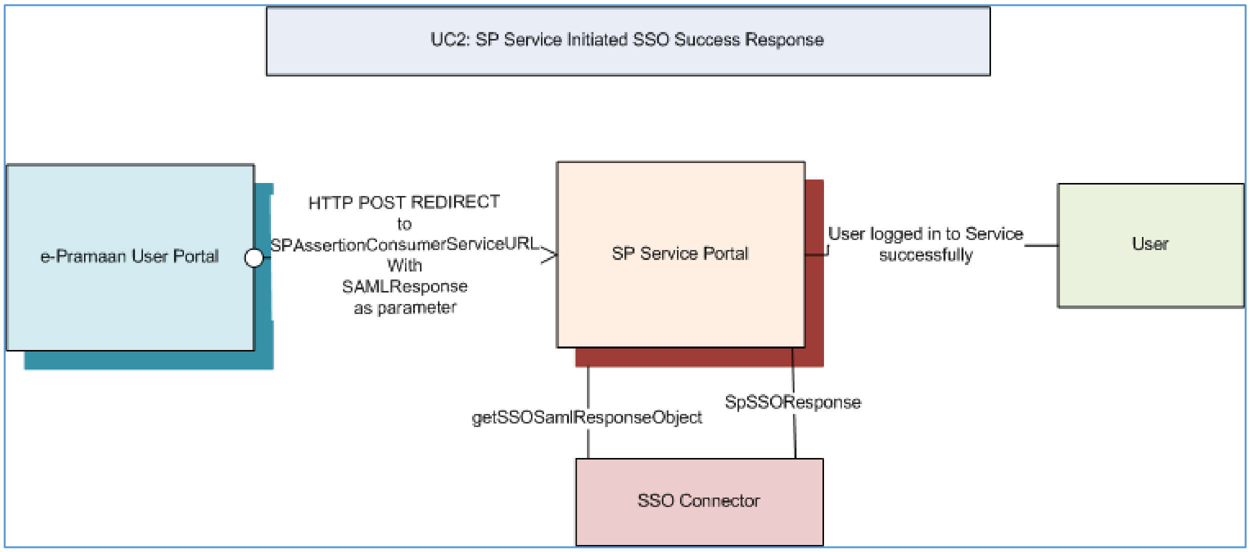
SSO request at SP will be created by the SSO-Connector component using SAML SSO Authentication Request Creator module. The parameters for AuthnRequest are populated from the epramaanconnector.properties file as per the mapping given below.

SL. No	Parameter	Value from epramaanconnector.properties

1	AssertionConsumerServiceURL	SPServiceHomePageURL+ SPAssertionConsumerServiceURL

12.2.2.2 SSO Success Consumer (HTTP POST)

The user, after successful authentication at e-Pramaan, will be redirected back to the SP service which initiated the communication. This redirect is a HTTP post redirect and the user credentials are provided by e-Pramaan in a SAML Response. The service at SP has to consume the response and make the decision whether to log-in the user or not. UC diagram for this is given below.


UC2: SP Service Initiated SSO Success Response
e-Pramaan User Portal
HTTP POST REDIRECT to SPAssertionConsumerServiceURL With SAMLResponse as parameter
SP Service Portal
User logged in to Service successfully
User
getSSOSamlResponseObject
SpSSOResponse
SSO Connector

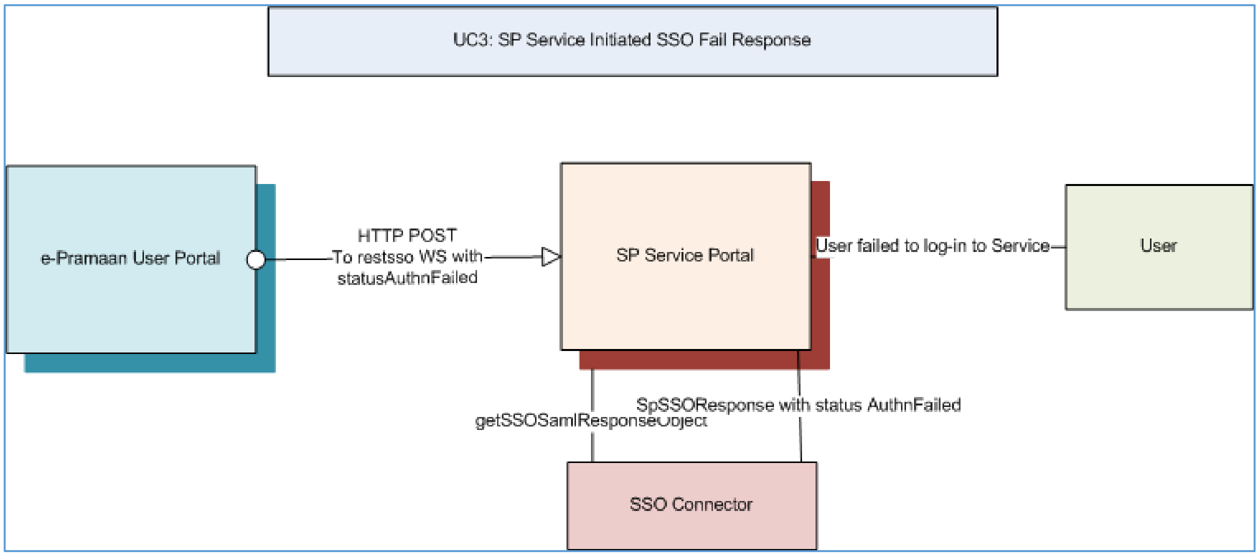
The SAML Response will be received by a consumer which decodes and processes the response. You have to create a page for that in the SP service. Sample code for decoding/processing the SAML Response will be given in Template.

12.2.2.3 SSO Failure Consumer (REST based WebService)

When a user tries to log-in through ePramaan, but fails to authenticate at e-Pramaan portal, the initiating SP will be intimated via a SAML Response. This saml Response will be send via RESTful Web service.

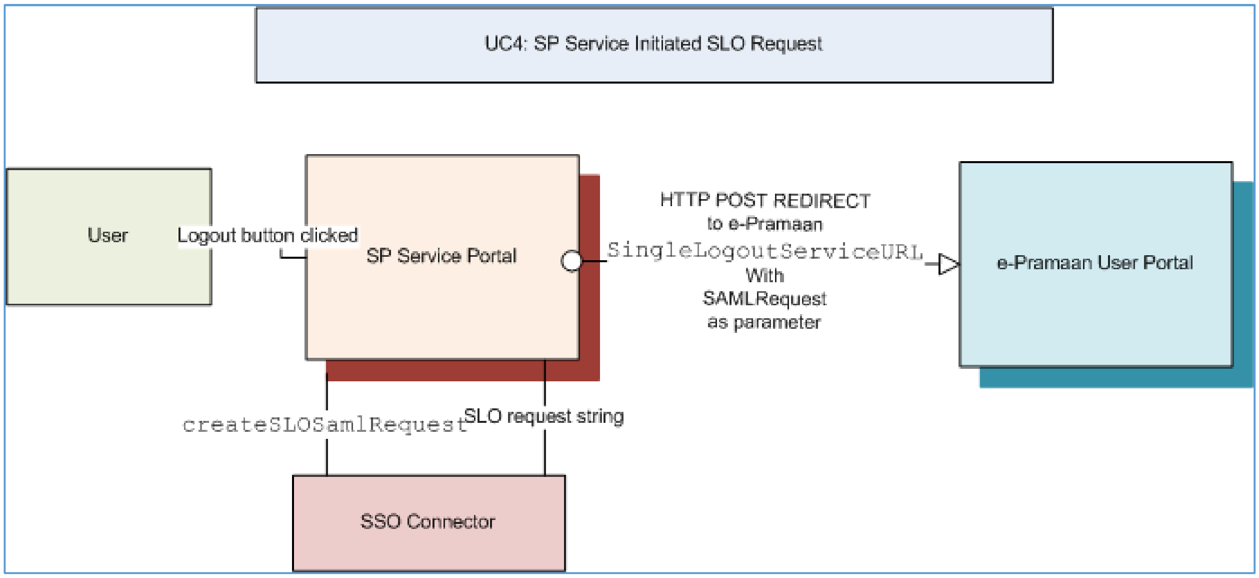
The integrating SP has to implement a web service for receiving this response. The response received in the SSO fail Web service may be used by the SP Service for logging/auditing purpose.

The Use-Case scenario is represented in the diagram below. Code sample for this ssofail Web Service will be given in Template



12.2.2.4 *Logout Request Creator (HTTP POST)*

If the user logs out of a service which he logged in through e-Pramaan, Single Logout is triggered. The user will be logged out from all the services he logged in through e-Pramaan. The UC diagram for SP Service initiated SLO is given below.

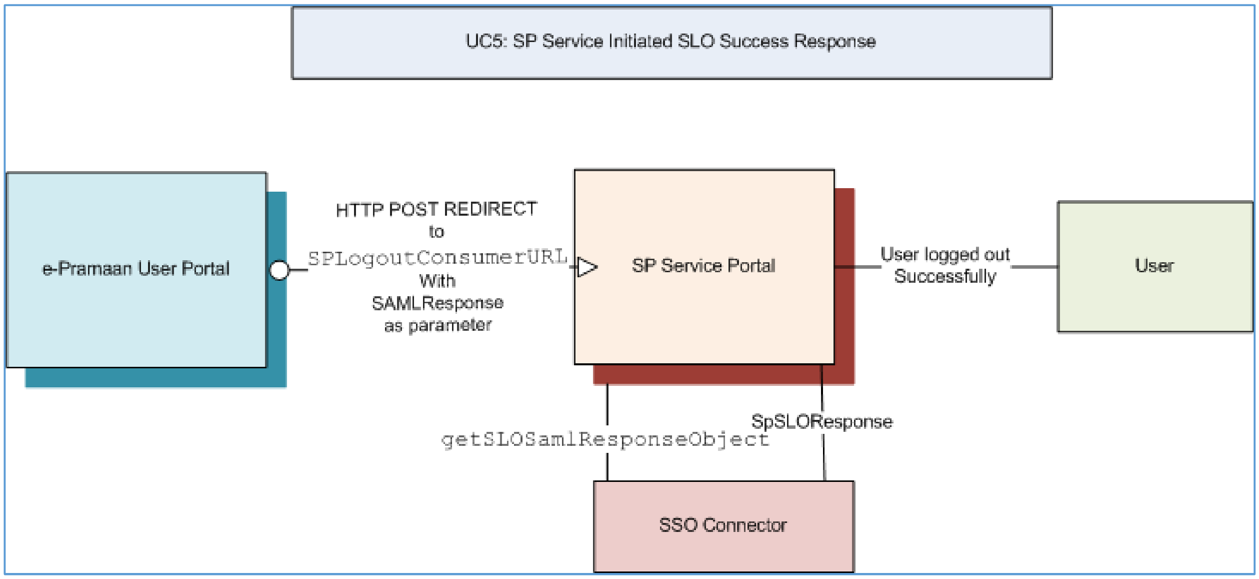


Logout Request will be created by the SP-SSO-Connector component based on the inputs from epramaanconnector.properties file and session identifiers present in http session. The fields are mapped as per the table given below.

Sr. #	Parameter	Value from epramaanconnector.properties
1	Destination	ePramaanURL+ SingleLogoutServiceURL
2	Issuer	Issuer
3	NameID	AadhaarNo / SP UserId received in the SAML SSO Success Response(this value should come from local session at SP Service)
4	SPNameQualifier	SPServiceHomePageURL
5	SessionIndex	SessionIndex received in the previous SAML SSO Success Response(This value should come from the local session at SP Service)

12.2.2.5 Logout Success Consumer (HTTP POST)

The user initiates SLO at SP Service by clicking the Logout button. After the Single logout is executed at e-Pramaan, status is send back to the initiating SP Service. The status may be success, if the logout was successful or the reason for failure in the case of failed SLO request. UC diagram for Logout Response Consumer is given below.

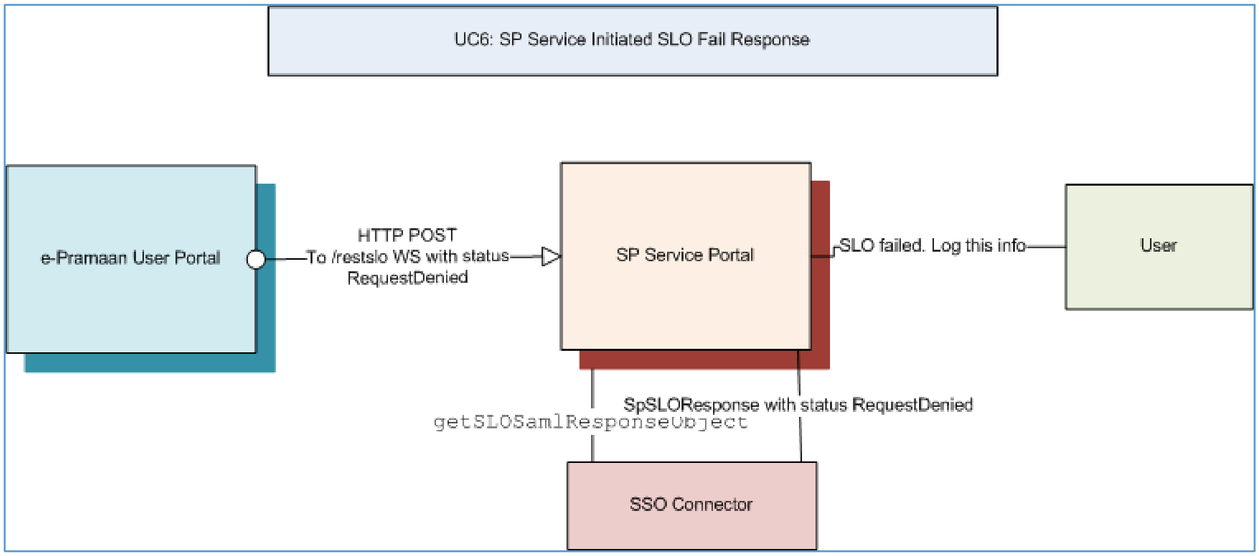

UC5: SP Service Initiated SLO Success Response
e-Pramaan User Portal
HTTP POST REDIRECT to SPLogoutConsumerURL With SAMLResponse as parameter
SP Service Portal
User logged out Successfully
User
getSLOSamlResponseObject
SpSLOResponse
SSO Connector

After consuming(processing) the Logout Request, SP may intimate the user whether single logout was successful or not.

12.2.2.6 *Logout Failure Consumer (REST based Webservice)*

Logout (SLO) button click at SP Service redirects the user to e-Pramaan. When logout attempt is successful, the user is redirected back to the initiating Service. But, when the logout fails at ePramaan, the user is not redirected back. The logout failure, in this case, is intimated via RESTful web service logoutfail Web Service.

The integrating SP has to implement the RESTful web service for logoutfail. The code sample for the same will be provided in the template.

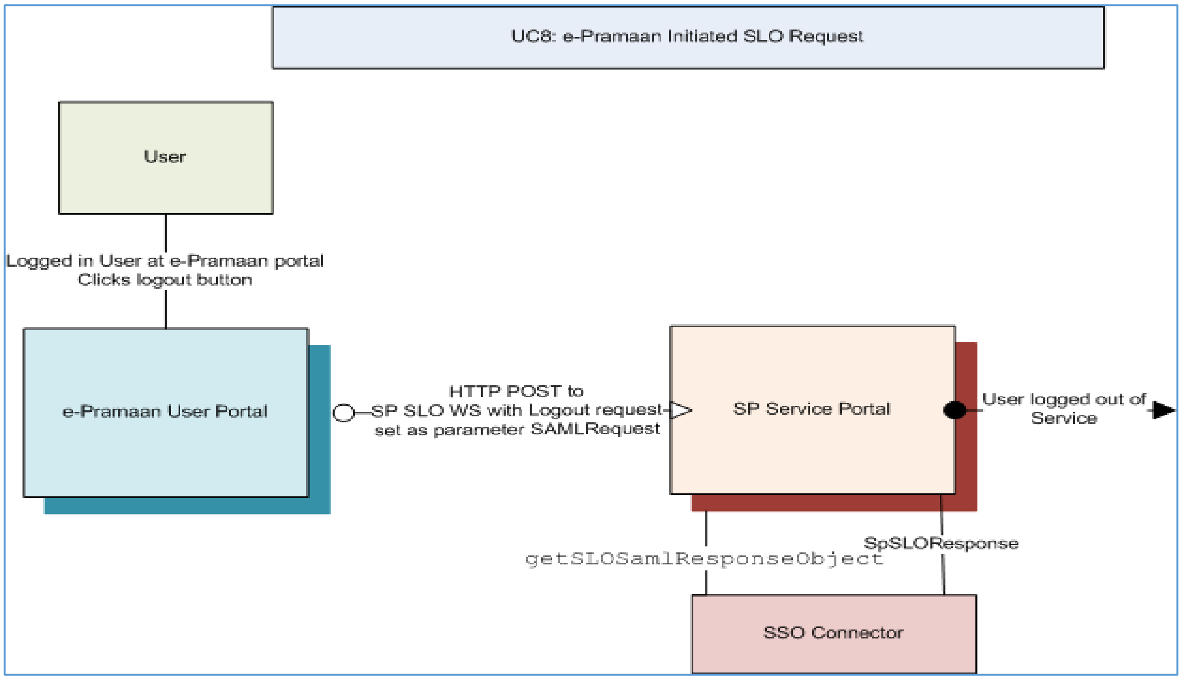

UC6: SP Service Initiated SLO Fail Response
e-Pramaan User Portal
HTTP POST
To /restslo WS with status
RequestDenied
SP Service Portal
SLO failed. Log this info
User
SpSLOResponse with status RequestDenied
getSLOSamlResponseObject
SSO Connector

12.2.2.7 *SLO Request Consumer (REST based Webservice)*

e-Pramaan allows user to log in to multiple services through e-Pramaan, in a single user session at e-Pramaan. Suppose that the user is logging out at the e-Pramaan website, all the associated services for the user has to be logged out. This is called e-Pramaan initiated Single Logout Service (SLO). e-Pramaan initiated SLO can be implemented only through RESTful web services.

In e-Pramaan initiated SLO, SP Service will receive a Logout Request from ePramaan. The service has to process and validate the request. If successfully processed the request, the service has to logout the user and terminate user session at SP Service. After this, the service has to send the status of the logout at SP, in a synchronous REST service response.

Use case diagram for this shown below.


UC8: e-Pramaan Initiated SLO Request
User
Logged in User at e-Pramaan portal Clicks logout button
e-Pramaan User Portal
HTTP POST to SP SLO WS with Logout request set as parameter SAMLRequest
SP Service Portal
User logged out of Service
getSLOSamlResponseObject
SpSLOResponse
SSO Connector

When a valid SLO request issued by e-Pramaan is received at SP Service, it is expected that the SP Service will (a) delete the local session and (b) send Logout response. This will ensure that the SP Service takes part in the SLO initiated by e-Pramaan. The request will be received in REST service call & response returned in the same sync call. SLO response will be created using the parameters from epramanconnector.properties as per the table given below.

SL .No	Parameter	Value from epramaanconnector.properties
1	Destination	ePramaanURL
2	InResponseTo	ID received in the LogoutRequest
3	Issuer	Issuer
4	Status	Not mapped to epramaanconnector.properties Can be any of the following 1)urn:oasis:names:tc:SAML:2.0:status:Success 2)urn:oasis:names:tc:SAML:2.0:status:RequestDenied

12.2.2.8 One Time Verification URL (HTTP POST)

If SP Service is registered with Service User ID mapping at e-Pramaan SP portal, than it is mandatory for the SP service to provide one time verification URL at the time of adding a service. The one time verification URL must validate the user at SP Service end and push the verification status to e-Pramaan REST WebService to complete the e-Pramaan User – Service User Id mapping.

When a user tries to access a SP Service for the first time then e-Pramaan HTTP POST redirects the user to SP service's verification URL with three request parameters. Request parameters are defined in the table below:

Sr. No.	Parameter name	Parameter value
	ssoToken	AES encrypted JSON object of ssoToken
	transactionId	Id to uniquely identify the transaction
	source	Constant Value i.e."ePramaan"

Note:- SP Service may use the data of SSOToken for pre-population / updation of user information.

12.2.2.9 Push back One Time Verification Response (Client call to REST based Webservice)

During One time verification, SP service will ask user to enter his login credentials and verifies the same.

When a user is successfully verified at SP Service during one time verification, the SP Service has to push back enrolment response to e-Pramaan. SP service will call e-Pramaan's Web service and push user's enrolment response for completing one time verification.

To push user's enrolment response the e-Pramaan Web service URL is:
https://up.epramaan.in/rest/epramaan/enrol/response. After this, user can access the SP Service by authenticating at e-Pramaan.

12.2.3 Technical details specific to implementation technology

12.2.3.1 Java Connector Details

Refer the document *Integration document - java specific.docx*

12.2.3.2 .NET Connector Details

Refer the document *Integration Document - .NET Specific.docx*

13. Appendix