IAM Authentication and Federation Service Integration Guide

Version 2.6

Table of Contents

This document describes IAM Authentication and Federation Service, along with the integration plan and requirements.

List of Figures

1. Introduction

Service providers are launching their services online, manual paper based transactions are substituted with the digital services. This approach is more economical, and very flexible for the end-users. However, these benefits come with the difficulty of managing and authenticating users online. User Registration and validation is a long and tedious phase, which consumes money and effort.

IAM comes to the picture to take away the burden of managing citizen and residents' digital identity. It is the Saudi National Identity Provider with solid way of identifying people online with unique digital identity. IAM has the ability to provide assurance to electronic service providers the identity of the individual seeking to obtain their services.

This document governs the process of integrating and using IAM services; it is categorized into two sections for the document purpose:

- Describe the IAM Authentication and Federation Service.
- Describe the integration process business and technical level.

2. Authentication and Federation Service

The authentication and federation allows authenticating end-users online based on service providers requests. This service does not deal with Authorization. The three actors involved within this service are illustrated in the diagram below:

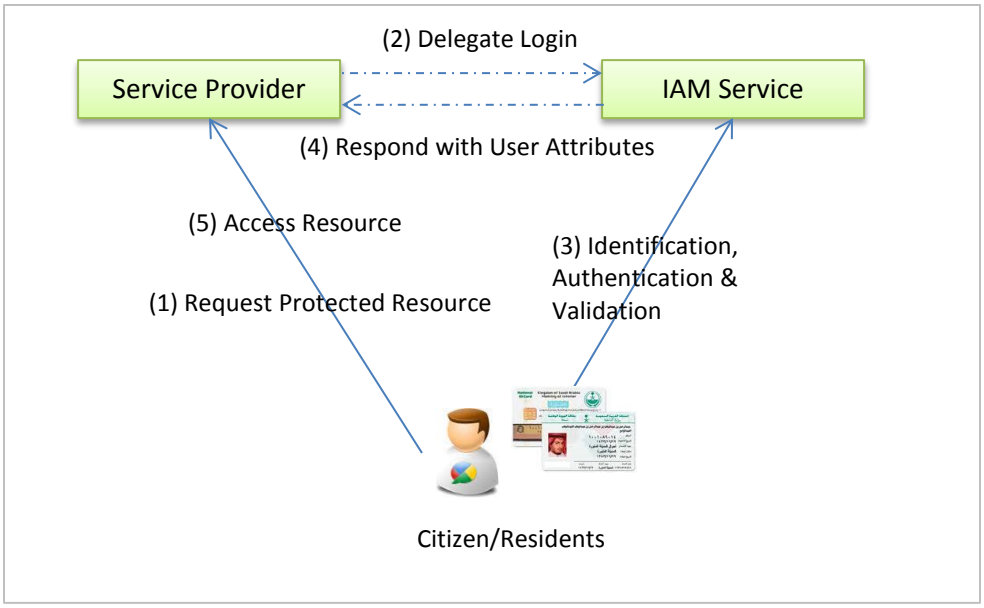


Figure 1: Different Actor involved in IAM Authentication Service

The communication between IAM and the Service Provider is not back-2-back and does not need any extra infrastructure requirements. “Delegate Login/Logout” is just a simple representation of the indirect communication between IAM & SP; practically the two entities exchange their data through the user browser.

This service deals the following functionalities:

- User Login:
  - Default Service Provider Authentication Sequence or Explicit Authentication Sequence
  - Force Authentication: Re-Authenticate the user again even if he was authenticated before.
  - Authentication Methods
    - Username Password Authentication
    - Mobile Authentication
    - Fingerprint Authentication
    - Email Authentication
    - IDCard Validation.

- IDCard PIN Authentication.
- Any combination of the above Authentication Methods.

- User Federation
  - Log once into IAM, Access All Service Providers
  - Step Up Authentication

- User Logout
  - Single Logout (SLO): where the user will perform the logout from the one service provider, and IAM takes care to dispatch the logout request to all service providers

- Manage Multiple Service Provider Resources
  - Different Authentication Policy
  - Force Authentication
  - Step Up Authentication (authentication upgrade)

2.1 IAM Login Scenario

In this scenario, the user is authenticated with his credentials (preconfigured in IAM such as IDCard and PIN number). The policy of the user authentication is defined as part of the integration process.

The user will have two options to Log In:

- Direct Login: through the Service Provider Login Process
- IAM Login: the user is authenticated and redirected to the Service Provider.

There is no direct communication between the IAM Service Servers and the Service Provider Servers as depicted below:

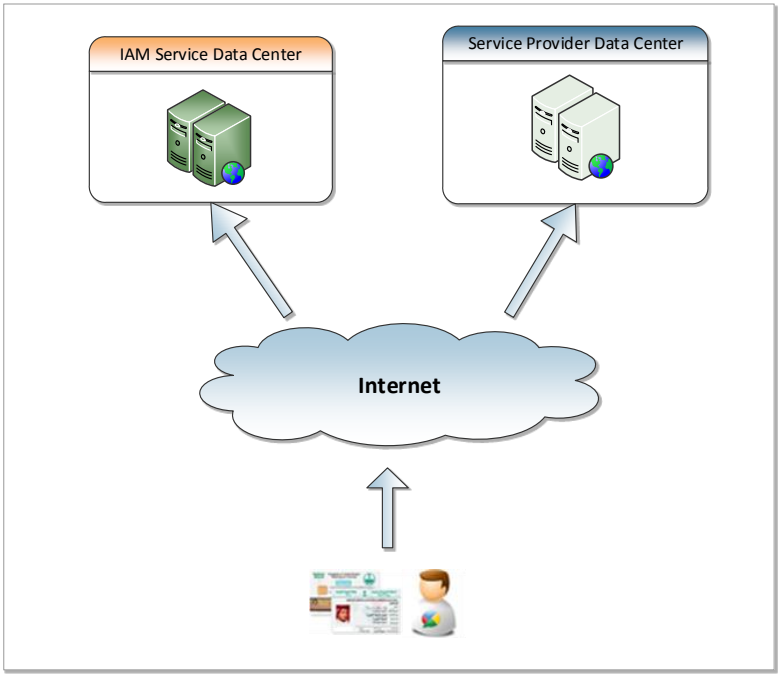


Figure 2: IAM & SP communication.

The communication between IAM Service to Service Provider is performed through the browser using standard redirects. No direct communication is required. This will make this solution much easier and practical since there is no impact on the infrastructure on both sides such as leased line, Firewalls rules changes, … etc.

2.1.1 User-Centric View after Integration

Based on the scenarios described earlier, below illustration of the final view that the user will see (MoI Portal is stated for the sake of clarity).

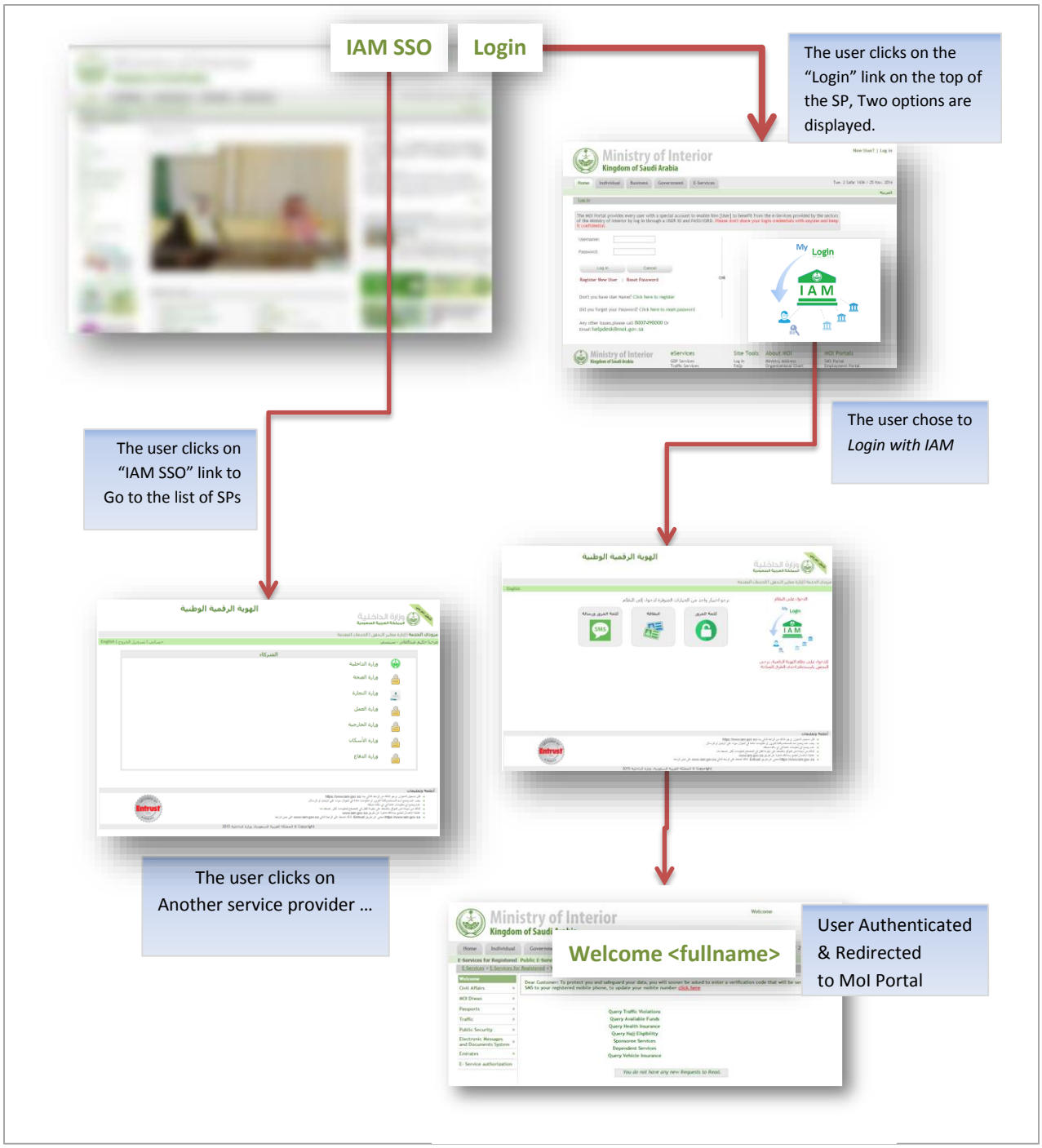


Figure 3: IAM / Service Provider Interactions from User Perspective (Example MoI Portal)

As part of the user experience, the language in which the page has been displayed must be consistent, which means that if the portal is displayed in English, IAM Service Login Screen must be in English. This point will be detailed more in the following section (integration Plan and Requirements).

The user is able to navigate between the service providers by clicking the link “IAM SSO” which will redirect him to “IAM Service Providers List”.

2.1.2 Technical Interaction Description

The following diagram depicts the interaction between a Service Provider, IAM system and the user; this is the technical details of the user-centric interaction illustrated above. The following sequence diagram illustrates IAM Authentication model:

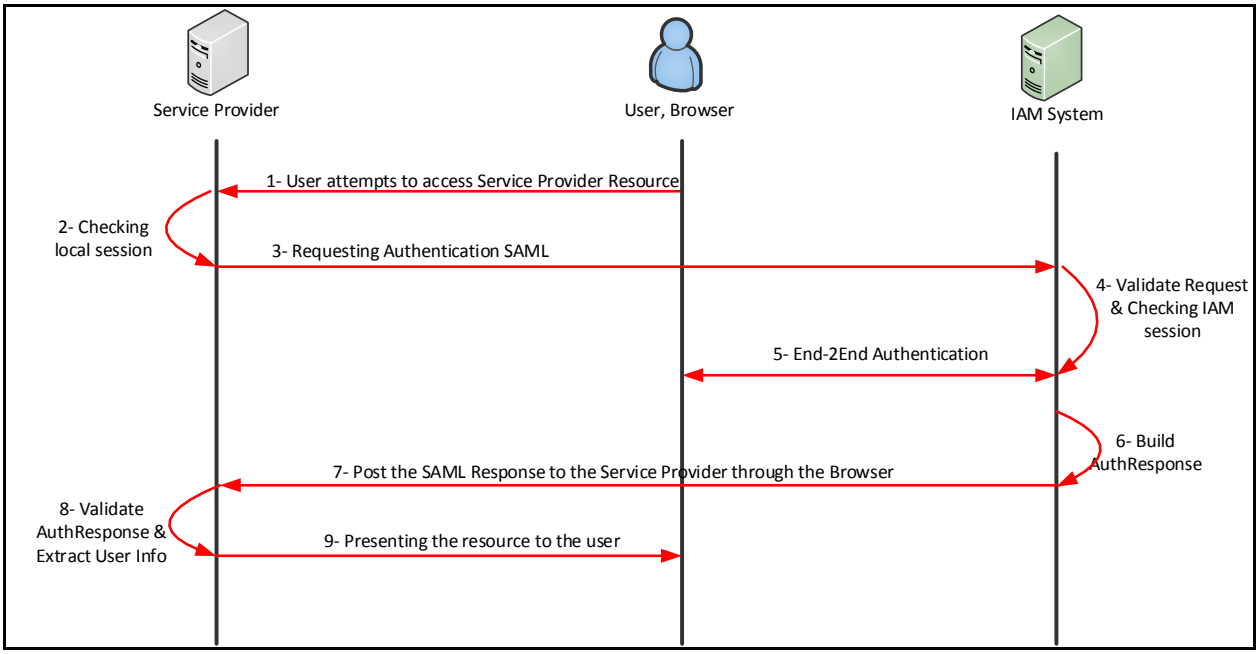


Figure 4: Login Scenario Sequence Diagram

The diagram is described below:

1. The user attempts to access a resource (on the main portal) on the service provider.
2. The service provider checks if the user is authenticated and possess valid local session:
    a. If the session exist and valid, the service provider checks if the user is authorized to access the resource.
    b. If the session doesn’t exist, the user is not authenticated and the service provider (if the default login of the service provider is kept as an option for the user, then the service provider displays the login page first with two options (direct login to the service provider and delegate login through IAM); once the user select the IAM Login Option,).

3. The service provider build a new authentication request, sign it and forwards the user authentication request to IAM by redirecting to the IAM system for authentication (HTTP Redirection).
4. IAM system checks if a global session (IAM session) exist:
    a. If the session exists go the step 6.
    b. If the session doesn't exist, go the next step.
5. IAM system do End-2-End authentication of the user (the authentication handshake can go through a lot of steps depending the authentication method to be in place). Once authenticated, a new IAM AuthSession is created for the user.
6. IAM system build a signed SAML authentication response containing user information
7. IAM system post the response to the service provider through the browser.
8. The service provider validates the authentication response and extracts all user attributes.

    a. It is important to store the signed SAML2 response coming from IAM in log files or database. In addition, it is recommended to log the SAML2 request as well.

    b. It is necessary to automatically check that the user has an account within the service provider repository; if not, the service provider has to treat this as auto-provisioning request and to do on-the-fly-registration of the user.

9. The service provider will serve the user and displays the requested resource.

User Validation

Implicitly the service validates the user against these controls:

1. Person Death: checks if the person is already dead. So somebody else is trying to use his card.
2. Person Suspended: the person is suspended.
3. Person Nationality Suspended (residents only): the nationality of the user is blacklisted.
4. Person Iqama Expired (residents only): the iqama has expired.
5. Person Final Exit (residents only): if the resident Iqama has been terminated.

Specific requirements of validation are subject to discussion and agreement. IAM is able to adapt to the service provider's needs (either it is less or more validations needed).

2.1.3 Federated Identity

Federated Identity (sometimes referred to NameID, NameIdentifier or AccountLinking) creates a persistent association between the IAM account and the service provider account. IAM is meant to be used on national scale and thus the National ID (Iqama ID) is the federated Id.

In some cases, when the returned NameId returned is random value that should be used for another NIC service integrated with IAM in back-2-back channel. The NameId in this case is considered as temporary token for the operation. The validation of the token can be found in the document describing the service/operation.

2.1.4 Authentication Request Details

The following describe the authentication request of the Service Provider containing the following main attributes:

a. Identity of the Requester (Service Provider Entity ID)
b. Validation data such as digital signature, timestamp
c. Required Authentication: explicit or implicit, force authentication.

The SAML2 authentication request sent from the service provider to IAM should be similar to:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" Destination="https://www.iam.gov.sa/samlsso"
ID="RB87E7DE8DE0DFA12B1FABC17B92F13401326CC6D" IssueInstant="2011-11-30T06:29:59Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
        <saml:Issuer>nicsp</saml:Issuer>
        <samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-
        format:persistent"/>
        <samlp:RequestedAuthnContext>
          <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
          </saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

The important information that composes an authentication request and the service provider should be aware of are:

- **Destination**: A URI reference indicating the IAM address to which this request has been sent. The default value: https://www.iam.gov.sa/samlsso
- **ProtocolBinding**: A URI reference that identifies a SAML protocol binding to be used when IAM returns the SAML <Response> message
- **Issuer:** The service provider name issuing the authentication request.
- **NameIDPolicy:** IAM will use the National ID as persistent identifier of the user.
- **AuthnContextClassRef:** A URI reference identifying the authentication context class that describe the authentication context by using the following mapping:

Authentication Methods (AuthnContextClassRef)	URI
Unspecified	urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified use the pre-configured authentication scheme
Username/Password	urn:oasis:names:tc:SAML:2.0:ac:classes:Password or urn:oasis:names:tc:SAML:2.0:ac:classes:ProtectedPassword
Username/Password with One Time Password	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
IDCard	urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

2.1.5 Authentication Response Details

The following describe the authentication response of IAM along with their main attributes.

1. IAM Identity: Identity of the IAM Authentication Service
2. Message Validity: validation data such as digital signature, timestamp, single use.
3. User Identity: users attributes are listed in the table below:

#	Attribute Name	Type	Description
1	nationalId	String	This is the user identifier represented by the National Id (Resident Id) SAML2 NameID or http://iam.gov.sa/claims/userid
2	lang	Enum	For Language Consistency/Preferred Language of the user (AR/EN) http://iam.gov.sa/claims/lang
3	arabicName	String	Arabic Full Name http://iam.gov.sa/claims/arabicName
4	englishName	String	English Full Name http://iam.gov.sa/claims/englishName
5	dobHijri	Date	Date Of Birth Hijri Example: 1487/06/12 http://iam.gov.sa/claims/dobHijri
6	dob	Date	Date Of Birth Gregorian Example: Tue Feb 30 03:00:00 AST 1987 http://iam.gov.sa/claims/dob
7	arabicNationality	String	Arabic Nationality http://iam.gov.sa/claims/arabicNationality
8	nationality	String	English Nationality http://iam.gov.sa/claims/nationality
9	nationalityCode	String	Nationality code, list of codes are in the Annex D. http://iam.gov.sa/claims/nationalityCode
10	gender	Enum	Male/Female http://iam.gov.sa/claims/gender
11	arabicFirstName	String	Arabic First Name http://iam.gov.sa/claims/arabicFirstName
12	englishFirstName	String	English First Name http://iam.gov.sa/claims/englishFirstName
13	arabicFamilyName	String	Arabic Family Name http://iam.gov.sa/claims/arabicFamilyName
14	englishFamilyName	String	English Family Name http://iam.gov.sa/claims/englishFamilyName
15	arabicFatherName	String	Arabic Father Name http://iam.gov.sa/claims/arabicFatherName
16	englishFatherName	String	English Father Name http://iam.gov.sa/claims/englishFatherName
17	arabicGrandFatherName	String	Arabic Grand Father Name http://iam.gov.sa/claims/arabicGrandFatherName
18	englishGrandFatherName	String	English Grand Father Name http://iam.gov.sa/claims/englishGrandFatherName

19	assuranceLevel	String (Optional)	Level of Assurance according to the authentication sequence and the status of the user registration http://iam.gov.sa/claims/assuranceLevel
20	cardIssueDateGregorian	Date	Gregorian Saudi Identity Card Issue Date or Iqama Issue Date Example: Tue Jan 20 03:00:00 AST 2015 http://iam.gov.sa/claims/cardIssueDateGregorian
21	cardIssueDateHijri	Date	Hijri Saudi Identity Card Issue Date or Iqama Issue Date Example: 1436/09/29 http://iam.gov.sa/claims/cardIssueDateHijri
22	IssueLocationAr	String	Card Issue Location, Example: Riyadh http://iam.gov.sa/claims/issueLocationAr
23	IssueLocationEn	String	Card Issue Location, Example: الرياض http://iam.gov.sa/claims/IssueLocationEn
24	iqamaExpirationDateH	Date	Hijri Iqama Iqama Expiration Date Example: 1436/09/29 http://iam.gov.sa/claims/iqamaExpirationDateH
25	iqamaExpirationDateG	Date	Gregorian Iqama Expiration Date Example: 2017/09/29 http://iam.gov.sa/claims/iqamaExpirationDateH

Note that the Service will provide extra user attributes upon request by Service Provider Team, compliant to NIC privacy policy. The users credentials are never sent to the Service Provider in direct or indirect way (proxy for instance), this includes the username, password, PIN, fingerprints, iris … etc.

The Service Provider (SP) must handle the authentication response messages from IAM using the HTTP-POST. The message returned by the IAM will look like:

```
<samlp:Response Destination="https://www.sp.com" ID="s2c2fe9d1393901b1ca3f5cd0d044082341a86ac43"
InResponseTo="RB87E7DE8DE0DFA12B1FABC17B92F13401326CC6D" IssueInstant="2011-11-30T06:30:04Z"
Version="2.0">
        <saml:Issuer>https://www.iam.gov.sa/samlsso</saml:Issuer>
        <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success“></samlp:StatusCode>
        </samlp:Status>

        <saml:Assertion ID="s2f0949aa62f4125340f337ec7d09d0fdc928c1512" IssueInstant="2011-11-
        30T06:30:04Z" Version="2.0">
        <saml:Issuer>https://www.iam.gov.sa/samlsso</saml:Issuer>

        <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        NameQualifier="IAM" SPNameQualifier="SPName "
        SPProvidedID="SPName">1155512312</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData
        InResponseTo="RB87E7DE8DE0DFA12B1FABC17B92F13401326CC6D" NotOnOrAfter="2011-11-
        30T06:40:04Z" Recipient="https://www.sp.com/Post"/></saml:SubjectConfirmation>
        </saml:Subject>

        <saml:Conditions NotBefore="2011-11-30T06:25:04Z" NotOnOrAfter="2011-11-30T06:35:04Z">
        </saml:Conditions>

        <saml:AuthnStatement AuthnInstant="2011-11-30T06:30:04Z"
        SessionIndex="s2f0949aa62f4125340f337ec7d09d0fdc928c1512">
        <saml:AuthnContext>
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password
        </saml:AuthnContextClassRef>
        </saml:AuthnContext>
        </saml:AuthnStatement>

        </saml:Assertion>
</samlp:Response>
```

The service provider verifies the response based on the following:

- **Destination**: A URI reference indicating the SP address to which this response has been sent.
- **Issuer:** The identity provider name issuing the authentication response.
- **StatusCode**: Specifies if the authentication succeed or failed.
- **Subject:** Specifies the user authenticated in IAM.

- **AuthnContextClassRef:** A URI reference identifying the authentication context class that describes the authentication context by using the precedent mapping.
- **IssueInstant & Conditions (NotBefore and NotAfter)**
- **Digital Signature:** XML Signature of the response using the IAM certificate.
- **SessionIndex:** linked between the authentication request and response.

In addition, it extracts the user's attributes included in the authentication response message (saml:AttributeStatement element). There is no need for extra messages are exchanged for attribute release; the service provider does not explicitly ask for attributes during the login process.

2.2 IAM Logout Scenario

In this scenario, the user has been authenticated to the first service provider, and has been federated into another one (or others ones) upon the user's access request.

The users can logout in two ways:

- By clicking logout from the service provider page.
- By clicking logout on IAM directly.

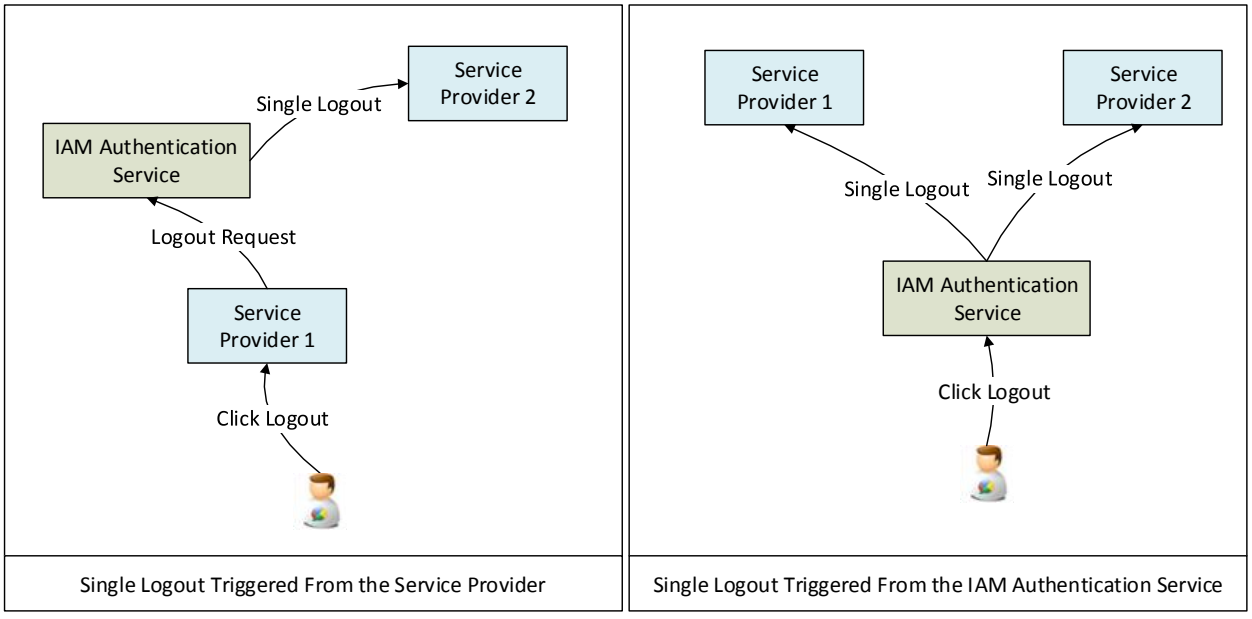


Figure 5: Single Logout Options

The requests and responses are very similar to the Login Scenario. In addition, IAM has implemented an easier way to handle the logout using direct URLs.

2.2.1 Technical Interaction Description

The logout process can be initiated based on two ways:

- User Logout from Service Provider Using SAML2
- User Logout from Service Provider Using Simplified Logout URI

Following detailed description of both forms of logout:

User Logout from Service Provider Using SAML2

The following is the process flow of logout from the service provider based on SAML 2 standard:

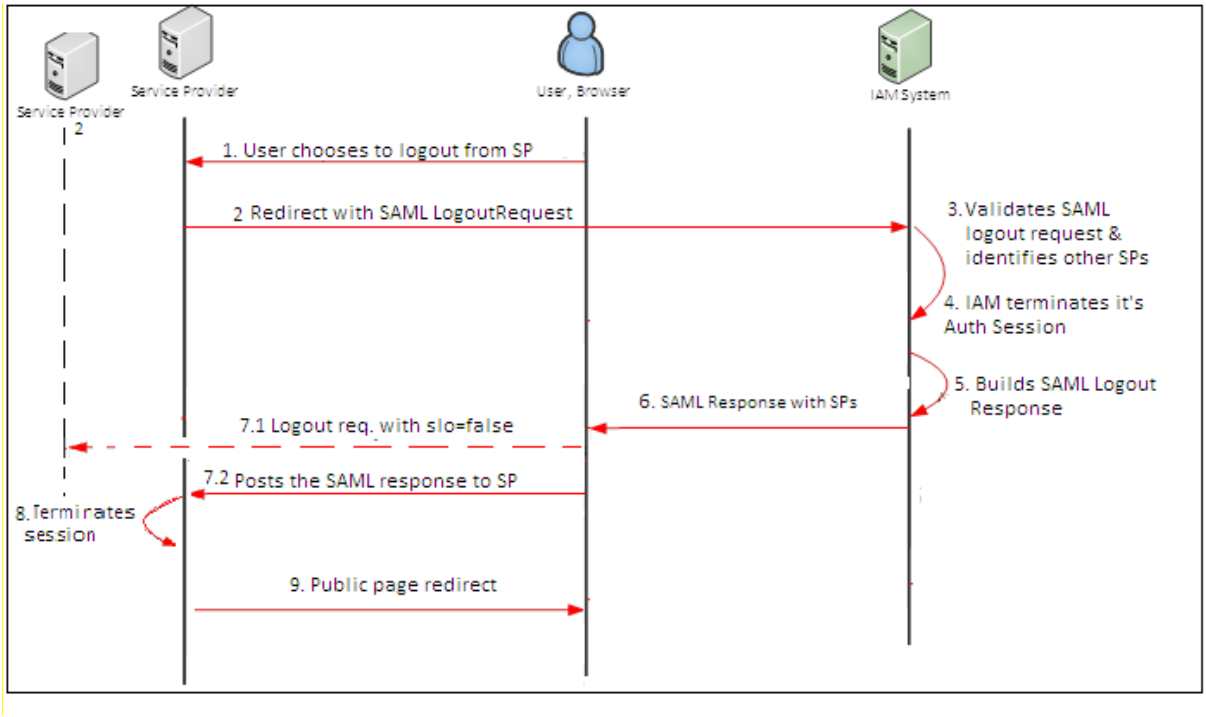


Figure 6: User Logout from Service Provider Using SAML2

1. The user chooses to logout from the service provider.
2. Service Provider generates a digitally signed SAML2 Logout Request and redirects to IAM logout URL "https://www.iam.gov.sa/samlsso".

3. IAM validates the SAML Logout Request; then determines, from the current user session, all the service providers that the user has logged on.
4. IAM terminates its Authentication session.
5. IAM builds a digitally signed SAML Logout Response message;
6. IAM sends back the signed response to the browser along with the list of service providers that are part of the logout operations.
7. The browser will do the following:

    7.1 First, the browser will send logout request to the listed SPs with request parameter 'slo=false'; each of these SPs terminates its own logon session for the current end user.

    7.2 Then, it forwards the Logout Response to the initiating SP.
8. The SP validates IAM SAML2 Logout Response and terminates its local session.
9. The originating SP redirects the user to the public page.

User Logout from Service Provider Using Simplified Logout URI

The following is the process flow of logout from the service provider using simple logout link:

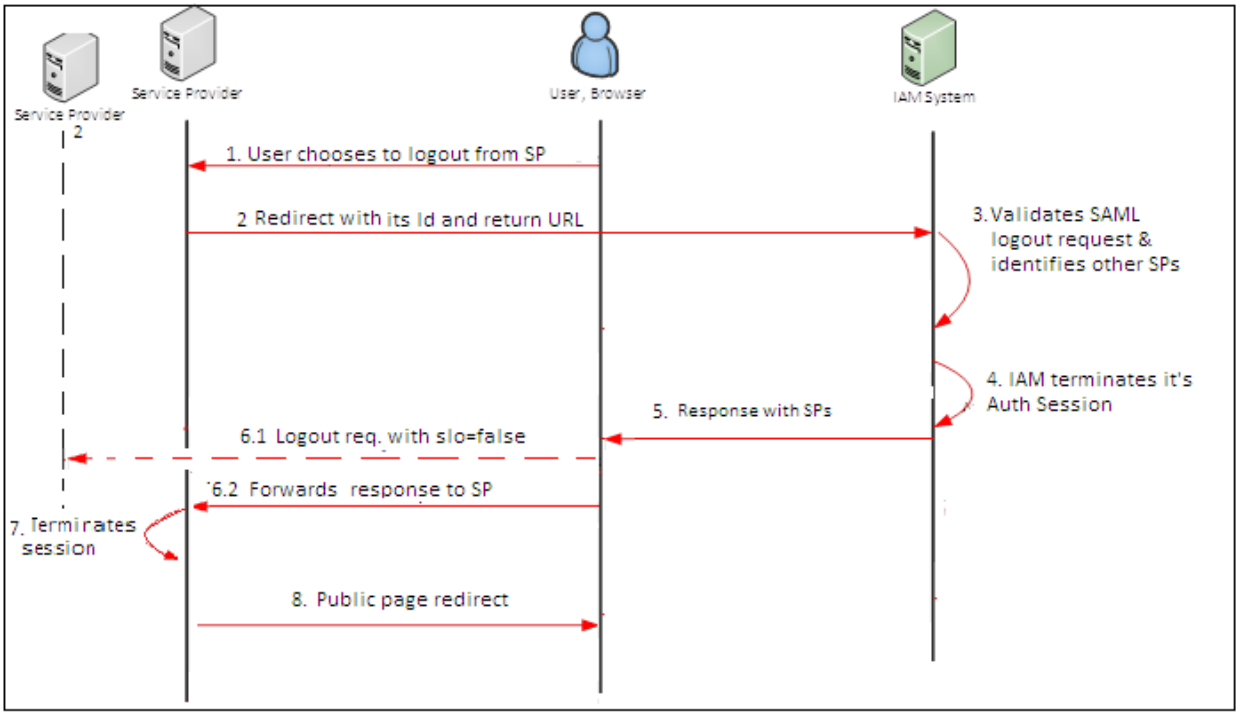


Figure 7: User Logout from Service Provider Using Simplified Logout URI

1. The user clicks on logout link from the service provider.
2. Service Provider logout the user locally by killing its session then redirects the user to IAM logout URL for e.g., "https://www.iam.gov.sa/samlsso?slo=true".
3. IAM validates the current Authentication Session; then determines, from the current user session, all the service providers that the user has logged on.
4. IAM terminates its Authentication session.
5. IAM sends back the response to the browser along with the list of Service Providers part of the logout operations.
6. The browser will do the following:
    6.1. The browser sends logout request to the listed service providers with request parameter 'slo=false'; each of these service providers terminates their logon session for the current end user.
    6.2. Then, it forwards the response to the initiating Service Provider.
7. The Service Provider terminates its local session.
8. The originating Service Provider redirects the user to the public page.

User Logout Initiated from IAM

The following is the process flow of logout from IAM (IDP logout):

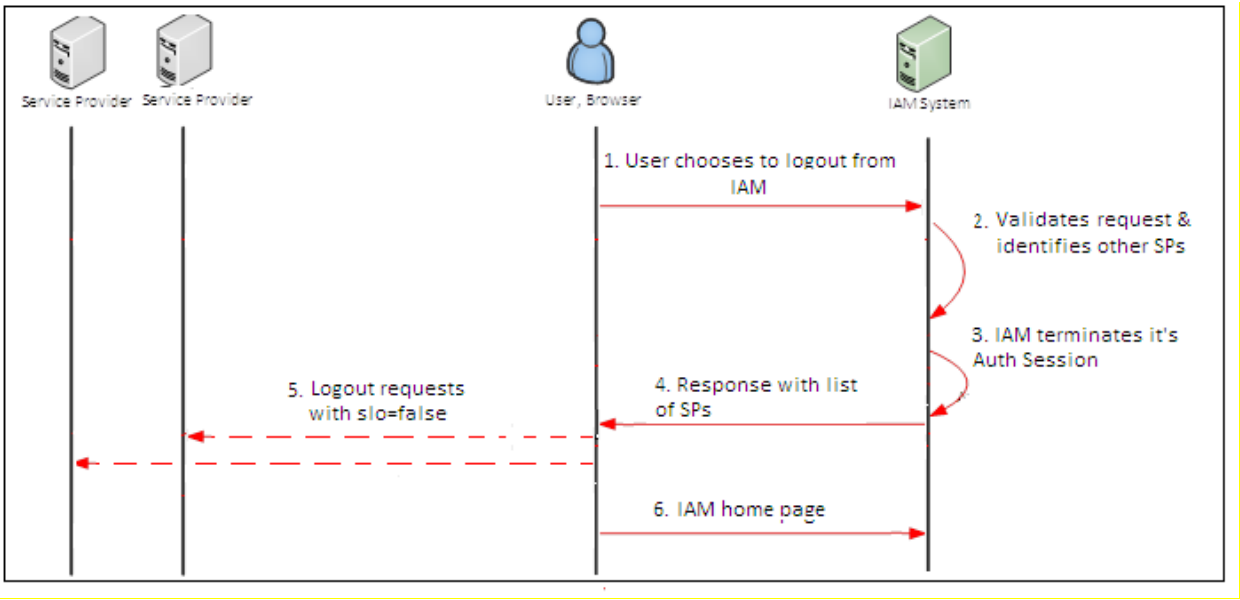


Figure 8: User Logout Initiated from IAM

1. The user clicks on the logout link on the IAM.
2. IAM validates the current Authentication Session; then determines, from the current user session, all the service providers that the user has logged on.
3. IAM terminates its Authentication session.
4. IAM sends back the response to the browser along with the list of Service Providers part of the logout operations.
5. The browser sends logout request to the listed service providers with request parameter 'slo=false'; each of these service providers terminates their logon session for the current end user.
6. Once the user is logged out from all the service providers, the user is taken to the IAM home page.

2.2.2 Logout Request/Response Details

- **Direct Logout**
  - **INPUT:** the URL is https://www.iam.gov.sa/samlsso?slo=true
  - **OUTPUT:** the URL issued to SP is https://serviceprovider.com.sa/logout?slo=false

- **SAML2 Logout Request**

- **INPUT**

The logout request sent from the service provider to IAM should be similar to:

```
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://www.iam.gov.sa/samlsso" ID="_cb32bak45d0sdg87d0gdf08fgd"
IssueInstant="2017-03-12T07:34:40.058Z" Reason="Single Logout" Version="2.0">
        <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        NameQualifier="nameQualifier">
        https://www.serviceprovider.com.sa/secure/Login</saml2:Issuer>

        <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-
        format:entity">1132077577</saml2:NameID>

        <saml2p:SessionIndex>s255bf14slkdfj324sg9087dfgd309458xlkdgjd03487
        </saml2p:SessionIndex>
</saml2p:LogoutRequest>
```

The important information that composes logout request and the service provider should be aware of are:

- **Destination:** A URI reference indicating the IAM address to which this request has been sent. The default value “https://www.iam.gov.sa/samlsso”
- **Issuer:** The service provider name issuing the logout request.
- **NameID:** IAM will use the National ID as persistent identifier of the user.
- **SessionIndex:** Session identifier that is sent with authentication response when SLO is enabled for the service provider.

- **OUTPUT**

The Service Provider (SP) must handle the logout response messages IAM using the HTTP-POST. The message returned by the IAM will look like:

```
<saml2p:LogoutResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://www.serviceprovider.com.sa/secure/Login"
ID="_cb32ba31418f1585dfbf3bbd6a5c8145" InResponseTo="_f05972ea60db4abac380567b0a758b46"
IssueInstant="2017-03-12T07:31:14.573Z" Version="2.0">
        <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-
        format:entity">https://www.iam.gov.sa/samlsso</saml2:Issuer>

  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#_cb32ba31418f1585dfbf3bbd6a5c8145">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
              <ds:DigestValue>qsBu2J6Jx6bPB/DeJCj6Z3V0siY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>eJGYy5pz70hlPaMKka7fKMMh+h36hI+qthKkUsYy777B67Hv/dhAr4hXIrYjQ=</ds:
        SignatureValue>
        <ds:KeyInfo>
              <ds:X509Data>
              <ds:X509Certificate>MIICNTCCAZ6gAwIBAgIES343gjANBgkqhkiG9w0BAQUFADBVMQswCQY
              Dc/E/Wq8uHSCo=</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
  </ds:Signature>
  <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
</saml2p:LogoutResponse>
```

The service provider verifies the response based on the following:

- **Destination**: A URI reference indicating the SP address to which this response has been sent to.

- **Issuer:** The identity provider name issuing the logout response.
- **StatusCode**: Specifies if the logout is succeed or failed.
- **IssueInstant:** The timestamp of the response.
- **Digital Signature:** XML Signature of the response using the IAM certificate.

2.3 Authentication Protocol Consideration

For reasons of security and interoperability, «SAML 2.0 Web Browser SSO Deployment Profile» is the only protocol to be used.

The messages exchanged are signed as a must (encryption is optional). Any non-signed request/response should be rejected (from IAM/Service Provider). The certificate used by the Service Provider is issued by IAM Team during Integration. In addition, IAM requires that the service provider uses HTTPS, and will only send authentication responses to HTTPS-enabled endpoints. The certificate used by the service provider for signing the authentication requests is issued during the Integration.

IAM will sign the SAML responses or assertion. The service provider must check the signature of incoming authentication responses to ensure that it is sent from IAM and must handle validation of the message (Response Signature Valid, Response Issuer Valid, Response Timeframe Valid, Single Use of Response, Request-Response IDs Matching). These kinds of checks are automatically handled by built-in SAML Service Provider Platform. Below diagram, illustrate the messages (along with signing/validation) between service providers and IAM Authentication Service.

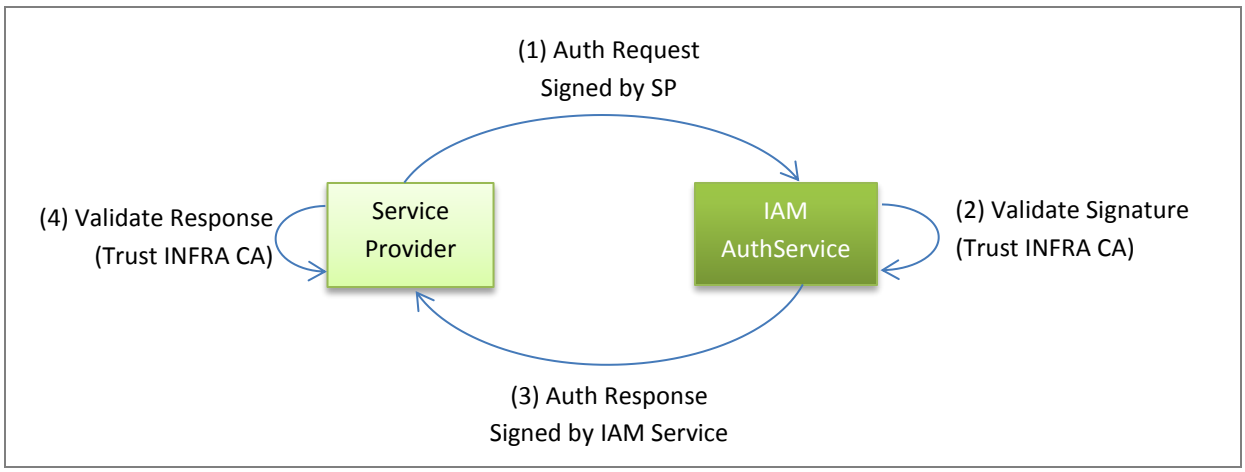
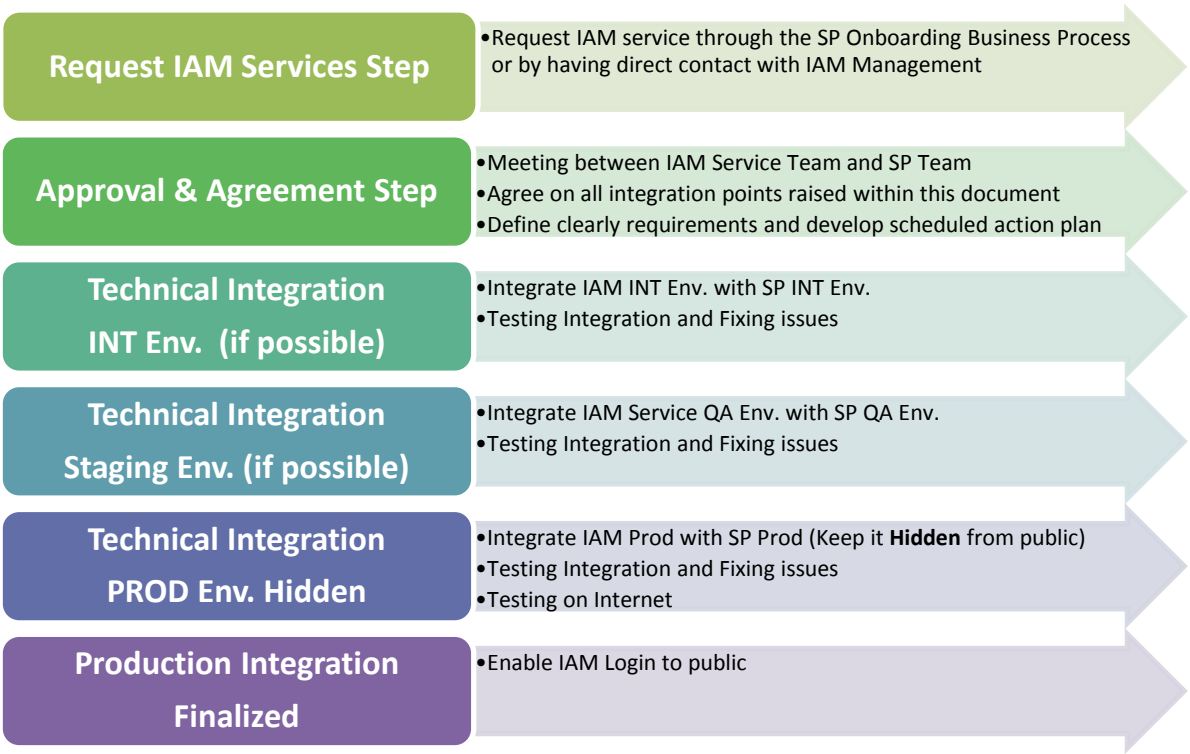


Figure 9: High Level Interaction between SP & IAM - Delegation

3. Integration Plan

The following diagram illustrates the integration plan. It is divided into the following steps:



Note: At the end of each step, the integration teams will meet and report the status to IAM/Service Provider management.

At the end of the integration effort, a report should be submitted to top management, this will make an end to previous step and launch the next one.

3.1 Request IAM Services Step

The IAM services can be requested in two ways:

Direct communication with IAM management: this is applied especially for government organization. Nevertheless, an owner has to be selected from the organization to be the point of contact and coordinator of the integration effort. He has to issue a formal request.

- The owner (or eligible person) of the company (or business entity) can request IAM services through https://www.iam.gov.sa/idpinit/ar/sp_onboarding.jsp. This screen will identify the requester and send his demand to IAM management.

In both cases, the requester has to provide the following Info, the first line is provided as sample:

#	Resource Alias	Description	Resource URL	User Target	Resource Policy		Technology / Platform	Current Authentication Scheme	Estimated Number of Transactions	User Attributes
					User Validation	Auth. Policy				
1	Sample Resource	This Sample Resource will allow the user to …	https://www.company.com/resource/sample	ALL	Registered or Activated, Alive or NA, Inside or Outside the country or NA,	IDCard + PIN OR Username Password + OTP	.Net / WebApp on IIS	Custom Login Page Relying on LDAP	220/400 Per Minutes	ALL

Where the:

- Resource URL: Service Provider URI, usually it is the main portal page.
- User Target: Citizen, Residents (Visitor are not yet handled)
- User Policy: Part of users validation Registered or Activated or NA, Alive or NA, Inside or Outside the country or NA,
- Authentication Policy (Sequences): Specify Options of any combination of the following IDCard, PIN, UP, Mobile, Email, Fingerprint
- Technology: .Net, Java, Python, PHP …
- Resource Platform: WebApp on IIS, WebApp IBM WebSphere AppServer, Oracle Portal, IBM Portal, SharePoint, …
- Current Authentication Scheme: Windows Integrated Logon, Custom Authentication Front, Custom Backend, Custom Membership Provider, Third Party SSO Solution, Users Repository
- Estimated Number of Transactions should be given in (Average/ Peak) Per Second or Minutes or Daily … Also, Peak Time
- User Attributes: the user attributes required by the service provider for each listed resource. The list of available attributes is defined in the service description in section 2.4.

The request goes through IAM Service Provider Onboarding Business Process Approval. The requester will be contacted and the next step can be carried on.

3.2 Approvals & Agreement Step

Once the request has been validated and got first approval, a more detailed discussion can take place. The main topics of this discussion is to finalize an agreement about all the details, management, business and technical level.

3.2.1 Management Discussions and Agreement

At the management level, discussions will cover the following points:

- Workshops and Meeting between IAM Service Team and Service Provider Team.
- Agree on all integration points raised within this document.
- Define extra requirements and develop scheduled action plan.
- Agree on the Process of raising Issues/Problems, new requirements or a change request.
- Define roles and responsibilities.
- Agree and Sign a contract by both parties including SLA.

3.2.2 Business & Technical Discussion and Agreement

At the technical level, the discussion will cover the following:

- **Service Provider Existent Architecture:**

The service provider team will explain the technical architecture and issue, this will serve for better understanding and planning.

- **Service Provider Requirements:**

The input here is the table filled by the service provider filled in the previous step:

- Discuss the resources to protect.
- Discuss Service Provider user attributes requirements.
- Discuss the required users' validation.
- Discuss the logout processes and requirements.
- Define Service Provider Policy:

- Default Authentication Method Required (Authentication Sequences Allowed) for desktop and mobile clients,
- Possibility to specify Authentication Method during the request,
- Federation Policy,
- Force Authentication,

- **Service Provider Integration**
  - Discuss the possibility to do the integration on Integration and Pre-production,
  - Discuss the SAMl2 authentication protocol enablement.
  - Discuss Authentication Request/Response Validations :
    - Digital Signature Validation
    - Timestamp Validation,
  - Login Options and how it will be presented to the User,
  - Discuss the language consistency,
  - Discuss the need for implement the auto-registration (on the fly registration),
    - After authentication in IAM, the user may not exist in the Service Provider repository. In this case, the service provider has to auto-register the user.
    - The Service Provider should not prompt the user for any information provided as part of SAML2 request.
    - The service provider should not request the user for any credentials (especially the password).
    - If the auto-registration of the user needs a password (because of platform or SDK limitation), the service provider needs to generate the password randomly just for the purpose of creating the profile and not for authentication purpose. That password should be random enough to not be used even by system administrator.
  - Service Provider Identity (Certificate) requirements (usage and storage),
  - Statistics of the SP Portal related to Login
    - Number of daily logins,
    - Number of login peak.

- **Service Provider Portal Platform Readiness,**

  Based on these discussions and walkthrough the integration guide, IAM and service provider teams will assess the technical readiness to start the integration especially:

  - Service Providers resources architecture relevant to integration,
  - SAML2 authentication protocol support.
  - Auto-Registration Support.
  - User Identifiers.

3.2.3 Establish Technical Integration Timeline

Once all of these points are agreed, the step ends by establishing the integration timeline and defining the actions required with clear estimates as preparation to the next step.

#	Owner	Actions	Estimate (Days)	Description
1	**SP/IAM**	Complete the Technical Readiness of the Service Provider and IAM	TBD	Implement the identified technical gaps on IAM and the service provider and follow up to fulfill all pre-requisites. These gaps were identified during the discussion of requirements and technical integration requirements.
2	**IAM**	Register the Service Provider in IAM with agreed policy	1	IAM Team will issue a certificate for the service provider and then create a profile for it within IAM More information about the service provider is collected at this step.
3	**SP**	Register IAM in Service Provider as Identity Provider	2-3	The configuration needed is SAML2 Web SSO Post Binding, All configuration details are listed below.
4	**IAM/SP**	Testing the Integration	5-10	End-2End-Testing & Fixing Issues.
5	**IAM/SP**	Get approval to move to next environment	TBD	finalize the integration if it is in production

3.3 Technical Integration Step

Applies to INT (if possible),to STAGING (if possible) and Production.

At this step, IAM and the service provider went through the integration guide and several workshops have taken place covering management, business and technical topics. In addition, IAM and the service provider have established the timeline to be executed which is the purpose of this phase. The timeline five items are more explained hereafter:

- Complete the Technical Readiness of the Service Provider and IAM.
- Register the service provider in IAM with agreed policy.
- Service Provider to register IAM as Identity Provider.
- Testing the Integration.
- Get approval to move to next environment.

3.3.1 Complete the Technical Readiness of the Service Provider and IAM

This step will make sure that the Service Provider has implemented the defined gaps and is technically ready to use IAM authentication service. This may need a development effort on the Service Provider side. Even though, it is difficult to cover all gaps but usually the following are highly recurrent:

- Enable SAML2 authentication protocol in the service provider platform. This depends on the technology and platform used by the SP. Annex C contains some platform guidelines on how to enable SAML2.
- Service Provider default user Identifiers: the SP has to do some changes on the user repository in case the service provider is not using the national Id (Iqama Id) as an identifier.
- Implement “On the fly registration application” process: Several use cases need to properly handled:
    - Authenticated user not registered. Prompt user to complete his info.
    - Authenticated user already registered. Information Correct: No action.
    - Information Incorrect: Update the user entry.
- Customize the Service Provider login page:
    - Customize the Service Provider Login Page to handle Local Login and IAM Login (Federated Login).

- Implement the Service Provider Logout interceptor: for single logout purpose. The link should contain slo parameter similar to https://www.sp.gov.sa/logout?slo=[true|false].
    - When the slo is false, the service provider will just logout locally.
    - When the slo is true, the service provider will issue slo request (using either the simplified way or SAML2 based).

3.3.2 Register the Service Provider in IAM with agreed Policy

IAM team will have all the information required to configure the service provider with the details.

- ✓ Resource URL: this is the link to the resource to be protected (ex. login page), usually it is the portal link.

  For Arabic, Example: https://www.sp.gov.sa/resource or https://www.sp.gov.sa

  For English, Example: https://www.sp.gov.sa/en/resource or https://www.sp.gov.sa/en
- ✓ Service Provider Entity Id: This URL is the name of the Service Provider,

  Example: https://www.sp.gov.sa/resource or https://www.sp.gov.sa
- ✓ Service Provider Assertion Consumer Service URL: ACS URL if the link to the process that is initiating the SAML2 Request and Receive the Authentication Response.

  Example: https://www.sp.gov.sa/resource/acs or https://www.sp.gov.sa/acs
- ✓ Service Provider Logout URL:

  Example: https://www.sp.gov.sa/resource/logout or https://www.sp.gov.sa/logout.
- ✓ Authentication Methods Options:

  Example: username and password with IDCard or username password with one time password.
- ✓ Signing Certificate:

  Every Service Provider will have a dedicated certificate used to digitally sign the authentication requests. IAM will provide a new certificate for the Service Provider based on the CSR (Certificate Signing Request) coming from the Service Provider. The creation of the associated RSA keypair should be done at the service provider side. IAM team will guide the service provider during the certificate issuance process.

Other information related to the UI is required to finish the configuration:

- ✓ Service Provider Name (Alias).
- ✓ Login Service Provider Image Arabic and English.
- ✓ Login Label Arabic and English.
- ✓ Login Description Arabic and English.

The images, labels and descriptions will be displayed to the user to let him know that he is authenticating for Service Provider.

During non-production integration such as Staging, the Service Provider configuration will be isolated but can still use IAM default URL.

3.3.3 Register IAM as Identity Provider in Service Provider

The IAM team will provide the IAM Entity Descriptor. For some platforms, this will facilitate the configuration by just importing this file when configuring the Identity Provider (sample is provided on Annex B). The Service provider has to register IAM as a default Identity Provider using the following information:

- Entity ID: https://www.iam.gov.sa/samlsso
- Destination URL: https://www.iam.gov.sa/samlsso
- Protocol: SAML 2 Web SSO Profile: with the following bindings:
  - Request: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-REDIRECT or urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.
  - Response: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
- Service Provider Signing Certificate:

  This certificate has been provided in the previous step based on the SP CSR. It will be used to sign SP authentication requests.

- IAM Certificate: Provided by IAM Support , it is used to validate responses signature coming from IAM.

- Certificates Chain: the INFRA CA and the ROOT CA certificate. These two certificates must be imported into the service provider application keystore and must be trusted. They serve to validate the SP signing certificate and the IAM certificate.
- Logout URL: https://www.iam.gov.sa/samlsso?slo=true
- SAML2 Logout URL: https://www.iam.gov.sa/samlsso
- Attributes mapping should be configured to map the user attributes coming from IAM to the repository attribute.

Note that the configuration of SAML2 is platform specific and is out of the scope of this document.

3.3.4 Testing the integration

During staging integration, an isolated SP configuration is created on IAM. The only constraint is that the user accessing SP staging environment has connection to IAM over internet. IAM Support Team will provide appropriate configuration. Note that there is no need for direct connectivity to perform the integration on the Staging environment (neither for production). Following diagram shows the user/developer/tester accessing both environments (IAM and SP).

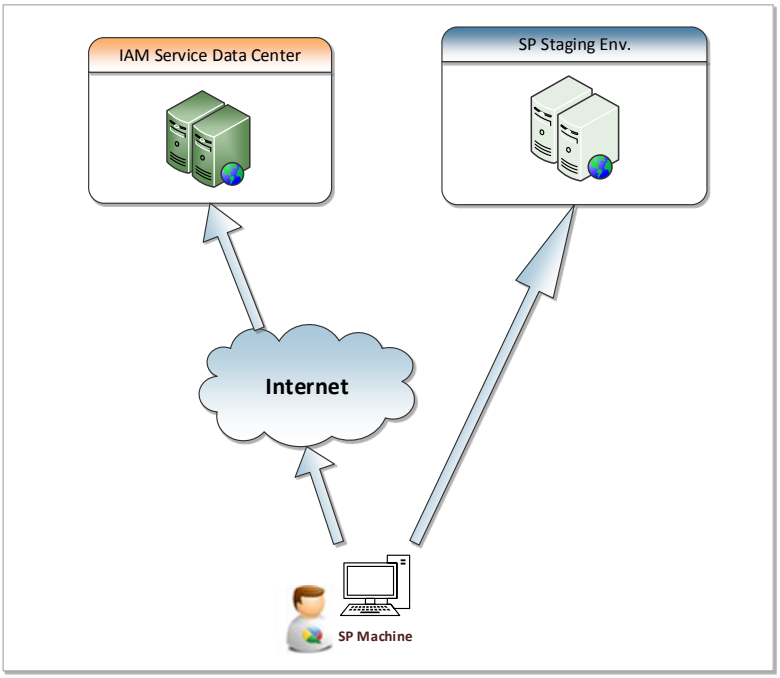


Figure 10: IAM/SP Staging Integration

The testing scenario is straightforward by applying the following test cases:

- Normal Login of an SP existent User on the Service Provider through SP Local Login.
  Expected Result: Successful Logged-In User to SP without soliciting IAM.
- Normal Login of an IAM registered user having an account in the SP repository.
  Expected Result: Successful Login (redirection to IAM and back to the SP), and update of the existing user profile or create a new one according to the SP policy (to separate IAM profiles and SP profiles).
- Normal Login of an IAM registered user NOT having an account in the SP repository.
  Expected Result: Successful Login on IAM and SP Auto-Registration Screen with user attributes populated and locked.
- A number of negative tests will be done according to IAM Test Plan.

A complete description of the test scenarios is included in the IAM Integration Checklist.

Important Notes

- ✓ The Arabic/English Switch should be consistent for the user. This means that if the user is on the Arabic page on the portal and wants to login. The Service Provider redirects him to the Arabic version of IAM Service and vice-versa. The possible values are EN, AR.

  The language consistency will be maintained during the authentication. “lang” HTTP attribute will be sent from the service provider to IAM as part of the Authentication Request (as additional parameter). The SAML2 response is sent from IAM back to the service provider including the “lang” as SAML2 attribute.

- ✓ Time Synchronization: the requests and responses are subject to number of validation. One of the validations is “TimeStamping”. The service provider will send the IssueInstant of the request; and the IAM Service will reply by the NotOnOrAfter timestamp of the response.

  If the both sides are NOT IN TIME Sync, there is a risk to reject the requests or the responses. Although the permissible time span (defaulted to 5 minutes) as difference between request and response, it is necessary to synchronize the two sides’ servers (servers where the requests are issued and consumed). Synchronizing with NTP server is recommended.

3.4 Production Integration Finalized

Once the integration is finalized, a report should be written summarizing all integration efforts and lessons learned. This document is presented to top management along with the recommendations for the next integration.

After receiving the integration report, IAM and Service Provider coordinators will agree on the right time to enable the Login through IAM. The IAM SLA contract will be signed by both parties.

4. IAM Contact Information

For any questions regarding IAM, contact:

- Saudi National Digital Identity Operations Manager: Mazen Alqarni (mhqarni@nic.gov.sa).
- Saudi National Digital Identity Applications PM: Nawaf AlMutairi (nmmutairi@nic.gov.sa).
- Saudi National Digital Identity Program Manager: Naji Algahtani (ngahtani@nic.gov.sa).

The IAM home page is: http://www.iam.gov.sa.

Annex A: Sample Authentication Messages

The authentication request sent from the service provider to IAM should be similar to:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" Destination="https://www.iam.gov.sa/samlsso"
ID="RB87E7DE8DE0DFA12B1FABC17B92F13401326CC6D" IssueInstant="2011-11-30T06:29:59Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
<saml:Issuer>https://www.iam.gov.sa/samlsso</saml:Issuer>
<samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent"/>
</samlp:AuthnRequest>
```

Figure 11: Sample Authentication Request

The important information that composes an authentication request and the service provider should be aware of are:

- **Destination**: A URI reference indicating the IAM address to which this request has been sent. The default value: http://www.iam.gov.sa/samlsso.
- **ProtocolBinding**: A URI reference that identifies a SAML protocol binding to be used when IAM returns the SAML <Response> message.
- **Issuer:** The service provider name issuing the authentication request.
- **NameIDPolicy:** Specifies the name identifier to be used to represent the requested subject. If omitted, then IAM will use the National ID of the user.
- **IssueInstant:** Authentication Request Issue Timestamp, used for validating the request by the IAM Service.

The authentication response sent from the service provider to IAM should be similar to:

Figure 12: Sample Authentication Response

```
InResponseTo="RB87E7DE8DE0DFA12B1FABC17B92F13401326CC6D" IssueInstant="2011-11-30T06:30:04Z"
Version="2.0"><saml:Issuer>nicidp</saml:Issuer><samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success“>
</samlp:StatusCode>
</samlp:Status><saml:Assertion ID="s2f0949aa62f4125340f337ec7d09d0fdc928c1512" IssueInstant="2011-
11-30T06:30:04Z" Version="2.0">
<saml:Issuer>nicidp</saml:Issuer><saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="nicidp"
SPNameQualifier="moiportal" SPProvidedID=" moiportal
">1234567890</saml:NameID><saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData InResponseTo="RB87E7DE8DE0DFA12B1FABC17B92F13401326CC6D"
NotOnOrAfter="2011-11-30T06:40:04Z"
Recipient="http://www.sp.sa/acs/saml2/Post"/></saml:SubjectConfirmation>
</saml:Subject><saml:Conditions NotBefore="2011-11-30T06:20:04Z" NotOnOrAfter="2011-11-
30T06:40:04Z">
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2011-11-30T06:30:04Z"
SessionIndex="s2f0949aa62f4125340f337ec7d09d0fdc928c1512"><saml:AuthnContext><saml:AuthnContext
ClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</saml:AuthnContextClassRef></saml:AuthnC
ontext></saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name=”NationalId” NameFormat=” urn:oasis:names:tc:SAML:2.0:attrname-format:basic”>
<saml:AttrubiteValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type=”xs:string”>
1234567890</saml:AttrubuteValue>
</saml:Attribute>
<saml:Attribute Name=”FullName” NameFormat=” urn:oasis:names:tc:SAML:2.0:attrname-format:basic”>
<saml:AttrubiteValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type=”xs:string”> full
name</saml:AttrubuteValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

The important information that compose an authentication request and the service provider should be aware of are:

- **Destination**: A URI reference indicating the SP address to which this response has been sent.
- **Issuer:** The identity provider name issuing the authentication response.
- **StatusCode**: Specifies if the authentication succeed or failed.
- **Subject:** Specifies the user authenticated in IAM.
- **NotOnOrAfter:** Authentication Response Timestamp used to validate the response by the service provider.
- **Attributes:** containing the information about the user authenticated.

Annex B: Sample Entity Descriptor Message Used During IAM Configuration

The authentication request sent from the service provider to IAM should be similar to:

```
<md:entitydescriptor entityid="https://www.iam.gov.sa/samlsso" validuntil="2023-09-23T06:57:15.396Z"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <md:idpssodescriptor protocolsupportenumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:keydescriptor use="signing">
      <ds:keyinfo>
        <ds:x509data>
          <ds:x509certificate>BASE 64 IAM Certificate</ds:x509certificate>
        </ds:x509data>
      </ds:keyinfo>
    </md:keydescriptor>
    <md:singlesignonservice binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
location=”https://www.iam.gov.sa/samlsso” />
    <md:singlesignonservice binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" location="
https://www.iam.gov.sa/samlsso" />

    <md:singlelogoutservice binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
location="https://www.iam.gov.sa/samlsso" responselocation="https:// www.iam.gov.sa/samlsso"/>

</md:idpssodescriptor>
</md:entitydescriptor>
```

Annex C: Frequently Asked Questions

#	What	Description
1	Enable SAML2 as Authentication Protocol on the Service Provider	On how enable SAML SSO, check the following: For IBM Websphere App. Server, version 7: http://publib.boulder.ibm.com/infocenter/ieduasst/v1r1m0/topic/com.ibm.iea.was_v7/was/7.0.0.23/Security/SAML_Web_SSO.pdf http://publib.boulder.ibm.com/infocenter/ieduasst/v1r1m0/index.jsp?topic=/com.ibm.iea.was_v7/was/7.0.0.7/SAML.html http://www-01.ibm.com/support/knowledgecenter/api/content/SSEQTP_7.0.0/com.ibm.websphere.base.doc/info/aes/ae/twbs_addsamltaisso.html?locale=en For IBM Websphere App. Server, version 8: http://www-01.ibm.com/support/knowledgecenter/#!/SSD28V_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_enablesamlsso.html For ASP.Net Web Applications, the following framework can be used: https://github.com/KentorIT/authservices Note that IAM team has an updated version of the KentorIT framework
2	Service Provider Certificate	Issue “Service Provider AuthRequest Signing Certificate” with the alias (CN=SP_DI) under InfraCA (from NIC PKI system). The resulting certificate must be in the Service Provider keystore (stored and used securely). Note: this certificate will be used to digitally sign the authentication requests.
3	On The Fly Registration	“On The Fly Registration” is the auto-registration of authenticated IAM users that are not on the SP repository.

Annex D: Nationality Codes

Following list of nationality codes:

CODE	Nationality Name Arabic	Nationality Name English
101	الامارات العربية	Arab Emirates
102	الاردن	Jordan
103	البحرين	Bahrain
104	سوريا	Syria
105	العراق	Iraq
106	عمان	Oman
107	فلسطين	Palestine
108	قطر	Country
109	الكويت	Kuwait
110	لبنان	Lebanon
111	اليمن	Yemen
112	اليمن الجنوبي	Southern Yemen
113	العربية السعودية	Saudi Arabia
114	يمني جنوبي-السلاطين	Yemeni the sultans
115	بني حارث	Bani Harith
116	الكويت -بدون	Kuwait - without
117	افراد القبائل	Member of the tribes
118	من سكان البحرين	Residents of Bahrain
119	قبائل مجاورة للعطفين	Tribes adj to Ataf
120	اجنبي بجواز سعودي	Alien KSA Passprt
121	فلسطيني بوثيقة مصرية	Palestinian Egyptian
122	فلسطيني بوثيقةلبناني	Palestinian Lebanese
123	فلسطيني بوثيقةاردنية	Palestinian Jordan
124	فلسطيني بوثيقةعراقية	Palestinian Iraqi
125	فلسطيني بوثيقة سورية	Palestinian Syria
126	وثيقة قطريه	document Syria
127	وثيقة عمانيه	The document Omani
128	وثيقة اماراتيه	The document EMIRIAN
129	وثيقة بحرينيه	Document Industry
130	عرب ثمانية وأربعون	Arabs 48
131	قبائل نازحة/الحليفه	Tribe/AlHal
132	اليمن - لحج	Yemen - pilgrimage
133	قبائل نازحة/الكويت	Tribes / Kuwait
134	غير كويتي	Unknown
135	غير بحريني	Unknown
136	غير قطري	Unknown
137	غير اماراتي	Unknown
138	غير عماني	Unknown
139	مقيم/نازح	

140	مقيم/مولود	
141	مقيم/طالب جنسية	
142	مقيم/أفراد القبائل	
143	مقيم/غير معروف	
144	مقيم/لا يحمل وثيقة	
145	قبيلة الصيعر	ALSAYAR
146	المناهيل والمهرة	ALMNAHIL AND ALMAHRH
201	تونس	Tunisia
202	الجزائر	Algeria
203	جيبوتى	Djibouti
204	السودان	Sudan
205	الصومال	Somalia
206	ليبيا	Libya
207	مصر	Egypt
208	المغرب	Morocco
209	موريتانيا	Mauritania
301	افغانستان	Afghanistan
302	اندونيسيا	Indonesia
303	ايران	Iran
304	باكستان	Pakistan
305	بنجلاديش	Bangladesh
306	بروني	Brunei
307	جمهورية ميانمار	Myanmar
308	تايلند	Thailand
309	تركيا	Turkey
310	جزر ملاديف	Maldives
311	روسيا الاتحادية	Russia
312	سنغافورة	Singapore
313	سري لنكا	Sri Lanka
314	الصين الوطنية	China National
315	الفلبين	Philippines
316	فيتنام	Vietnam
317	كمبوديا	Cambodia
318	كوريا الجنوبية	South Korea
319	ماليزيا	Malaysia
320	نيبال	Nepal
321	الهند	India
322	هونج كونج	HONG KONG
323	اليابان	Japan
324	بهوتان	Bhutan
325	الصين الشعبية	China
326	قبرص	Cyprus
328	كوريا الشمالية	North Korea
329	لاوس	Laos
330	منغوليا	Mongolia

331	ماكاو	Macao
332	تركستان	Turkistan
333	مقيم بلوشي	NULL
334	بخارستان	Bucharest
335	القبائل النازحة	Tribes emigrated
336	كازاخستان	Kazakhstan
337	ازبكستان	Uzbekistan
338	تركمانستان	Turkmenistan
339	طاجكستان	Tajikistan
340	قرغيزستان	kyrgyzstan
341	سقطرة	Socotra
342	مهرة	Muhrah
343	اذربيجان	Azerbaijan
344	الشاشان	Chechnya
345	داغستان	Dagestan
346	انقوش	Anquosh
347	تتارستان	Tatarstan
348	مكررلقرغيزيا لايستخدم	Kyrgyzstan not used
349	تيمور الشرقية	East Timor
350	مقيم	Resident
351	ميانمار/مقيم	NULL
352	ميانمار/جواز باكستان	-
353	ميانمار/جوازبنجلا دش	-
401	اثيوبيا	Ethiopia
402	اوغندة	Uganda
403	بوتسوانا	Botswana
404	بورندي	Burundi
405	تشاد	Chad
406	تنزانيا	Tanzania
407	توجو	Togo
408	جابون	Answer
409	غامبيا	Gambia
410	جزر القمر	Comoros
411	جنوب افريقيا	South Africa
412	ناميبيا	Namibia
413	بنين	Benin
414	رواندا	Rwanda
415	زمبابوي	Zimbabwe
416	زائير	Zaire
417	زامبيا	Zambia
418	ساحل العاج	Ivory Coast
419	السنغال	Senegal
420	سيراليون	Sierra Leone
421	غانا	Ghana

422	غينيا	Guinea
423	غينيابيساو	Guinea Bissau
424	بوركينافاسو	Burkina Faso
425	الكاميرون	Cameroon
426	الكونغو	Congo
427	كينيا	Kenya
428	ليسوتو	Lesotho
429	ليبيريا	Liberia
430	مالي	Mali
432	ملاوي	Malawi
433	موريشيوس	Mauritius
434	موزمبيق	Mozambique
435	نيجيريا	Nigeria
436	النيجر	Niger
437	افريقيا الوسطى	Central Africa
438	انجولا	Angola
439	الراس الاخضر	Cape Verde
440	غينيا الاستوائية	Equatorial Guinea
441	ملاجاسي	Mlajasi
442	ساوتومي/برنسبى	Sao Tome/FranceBank
443	جزر سيشل	Seychelles Islands
444	سوزيلاند	Swaziland
445	بوفثاتسوانا	Bovthatswana
446	رينيون	Reunion
447	ترانسكي	Transkei
448	فيندا	Venda
449	ارتيريا	Eritrea
450	دول افريقية اخري	Other African States
451	سانت هيلانة	Saint Helena
452	جزيرةمايوت	Comorian island
453	جمهورية جنوب السودان	Republic of South
454	كاب فيرد	CAPE VERDE
501	اسبانيا	Spain
502	البانيا	Albania
503	المانيا	Germany
504	ايرلندا	Ireland
505	ايطاليا	Italy
506	المملكة المتحدة	United Kingdom
507	البرتغال	Portugal
508	بلغاريا	Bulgaria
509	بلجيكا	Belgium
510	بولندا	Poland
511	رمزقديم تشكوسلوفاكيا	old to Czechoslovak
512	الدانمارك	Denmark

513	رومانيا	Romania
514	السويد	Sweden
515	سويسرا	Switzerland
516	فرنسا	France
517	فنلندا	Finland
518	صربيا	SERBIA
519	هولندا	Netherlands
520	يوغسلافيا	Yugoslavia
521	اليونان	Greece
522	اندورا	Andorra
523	النمسا	Austria
524	الجبل الأ سود	MONTENEGRO
525	هنغاريا	Hungary
526	ايسلندا	Iceland
527	ليختنشتين	Liechtenstein
528	لوكسمبورغ	Luxembourg
529	مالطا	Malta
530	موناكو	Monaco
531	النرويج	Norway
532	سان مورينو	San Moreno
533	مدينة الفاتيكان	Vatican City
534	جبل طارق	Gibraltar
536	اوكرانيا	Ukraine
537	روسيا البيضاء	Byelorussia
539	ارمينيا	Armenia
540	مولدافيا	Moldova
541	جورجيا	Georgia
542	ليتوانيا	Lithuania
543	استونيا	Estonia
544	لاتفيا	Latvia
545	البوسنة والهرسك	Bosnia / Herzegovina
546	كرواتيا	Croatia
547	سلوفينيا	Slovenia
548	صربيا والجبل الأسود	Serbia / Montenegro
549	مقدونيا	Macedonia
550	كوسوفوا	Kosovo
551	رمزقديم للجبل الاسود	code to Montenegro
552	تشيك	CZECH REPUBLIC
553	سلوفاكيا	Slovakia
554	جزر فيرو	Faroe Islands
555	ميتروبوليتان فرنسية	FRANCE METROPOLITAN
601	الولايات المتحدة	United States
602	الارجنتين	Argentina
603	بربادوس	Barbados

604	البرازيل	Brazil
605	بنما	Panama
606	ترينداد وتوباجو	Trinidad and Tobago
607	جامايكا	Jamaica
608	جوانا	Joanna
609	فنزويلا	Venezuela
610	كندا	Canada
611	كولمبيا	Columbia
612	جزر البهاما	Bahamas
613	كوستاريكا	Costa Rica
614	كوبا	Cuba
615	دومينيكا	Dominica
616	جمهورية دمينكان	Republic Dominica
617	السلفادور	El Salvador
618	جرانادا	Granada
619	جواتيمالا	Guatemala
620	هايتي	Haiti
621	هوندوراس	Honduras
622	المكسيك	Mexico
623	نيكاراجوا	Nicaragua
624	سانت لوسيا	Saint Lucia
625	سان فينسنت	Saintt Vincent
626	بوليفيا	Bolivia
627	شيلي	Chile
628	اكوادور	Ecuador
629	باراجواي	Paraguay
630	بيرو	Peru
631	سورينام	Suriname
632	اوراجواي	Orajoa
633	س بييري وميكويلن	Saint Pierre Miquel
634	جرينلاند	Greenland
635	بيليز	Belize
636	بيرمودا	Bermda
637	ج الترك والقوقاز	Turk/Caucasus Island
638	سان كريستوفرنيفز	San Cristovernivz
639	انجويلا	Anguilla
640	انتيكوا	Antiques
641	ج فيرجن البريطانية	British Virgin
642	جزر كايمون	Cayman Islands
643	مونت سيرات	Monte Sirat
644	جيودي لوب	Gyude Lube
645	مارتينيكو	Martinico
646	عروبا	Arabism
647	بونيري	Bonaire

648	كيوراكو	Curako
649	سان استاتيوس	San Astatios
650	سابا	Saba
651	سان مارتين	San Martin
652	بورتوريكو	Puerto Rico
653	ج فيرجن الامريكية	Virgin Islands of US
654	جزر فاكلاند	Falkland Islands
655	جيانا الفرنسية	French Guyana
656	الامم المتحدة	United Nations
657	جزر كوك	Cook Islands
659	باربودا	Barbuda
660	انتيل الهولندية	NETHERLANDS ANTILLES
661	جزر كوكوس	COCOS ISLAND
662	البريطانية في المحيط	BRITISH INDIAN OCEAN
663	سانت كيتس ونافيس	SAINT KITTS & NEVIS
664	جنوب جورجيا	SOUTH GEORGIA
701	استراليا	Australia
702	نيوزيلندا	New Zealand
703	بابوا نيوغينا	Papua yoga
704	نيو	New
705	انتاركتيكا	Antarctica
706	جزر نورفولك	Norfolk Island
707	توكيلاو	Tokelau
708	جزيرةكريسماس	Christmas Island
709	جزيرةكوكو-كيلنج	koko Island- Kellenj
710	فرنسا الجنوب القطبية	FRENCH SOUTH
711	جزيرة هيرد وماكدونلد	HEARD DONALD ISLANDS
712	جزر بيتكايرن	PITCAIRN ISLANDS
801	جزر فيجي	Fiji Islands
802	كيريباتي	Kiribati
803	نورو	Nauru
804	جزر سليمان	Solomon Islands
805	تونجا	Tonga
806	توفالو	Tuvalu
807	فانيوتو	Vanuoto
808	ساموا الغربية	Western Samoa
809	ساموا الامريكية	American Samoa
810	جوام	Guam
811	جزر ماريانا	Mariana Islands
812	ميكرونيسيا	Micronesia
813	جزر ماريشال	Marechal Islands
814	بيلو	Belo
815	بولينيسياالفرنسية	French Polynesia
816	جزر والس وفوتونا	Islands Wallis

817	كاليدونيا الجديد	New Caledonia
818	مدغشقر	Madagascar
819	قبيلة بالعبيد	Balobid
820	قبيلة النسي	NULL
821	قبائل مجاورة للعبر	TRIBES ADJACENT
822	قبيلة الحرث	NULL
823	قبيلة نهد	NULL
824	جزر مينور	US MINOR ISLANDS
825	مقيم اجنبي - الاشاجعة	NULL
826	مقيم اجنبي - العدوان	NULL
900	غير معروف	Unknown
901	اخرى	OTHER

Annex E: Service Provider Integration through Partner Guidelines

- Regular Audit on the partner system will be conducted by IAM Team.
- The partner should send the service provider URL (issuer or entityId) within the Audience attribute as part of the authentication request.
- The partner should comply with the integration guide.
- Service Providers Integrated with the partner should use a certificate issued from NIC PKI.
- The partner must digitally sign the response coming from IAM before send it to service provider. The certificate used for signing the response is the same certificate used for signing the request, and it should be issued from NIC PKI.
- The partner should store request/response coming/going to service provider for at least one year.
- Any integration with a new service provider should be in coordination of IAM.
- Authentication responses are sent to specific service provider (identified by audience) through the partner and cannot be re-used for another one.
- The federation/SSO should be handled by IAM and not by the partner. This is to make sure that the federation policy within is not compromised.
- The partner is responsible for validation using the IAM Service Provider Checklist of the integration and regular audits with service providers. IAM Team may participate in this activity.