**Service Name : Single-Sign-On(SSO)**

**Number Of API : 3**

**List Of API:**

1. IDP Login
2. Wizard Login
3. Dashboard Login

**OISF Core Service Definition**

**Core Service Name: ‘IDP Login’**

**Service Metadata Definition**

|  |  |  |
| --- | --- | --- |
| **Serial No** | **Service Information** | **Description** |
| 1 | Reference Number | 01.01.0001.0101 |
| 2 | Service Name | IDP Login |
| 3 | Description of Service | Third party application will be able to authenticate and log in a user through identity server |
| 4 | Owner | Oisf |
|  | Output type (Data/Service) | Service |
| 5 | Service Type ( Core/Shared) | Shared |
| 6 | Service Invoking Parameter | 1. User name in English 2. Password in English |
| 7 | Mandatory Fields for service Invocation | 1. User Name in English 2. Password in English |
| 8 | Data Reference Model (DRM) | See 01.02.0001.0101 of Data Standard |
| 9 | Application Integration Reference Model (AIRM) | See 01.03.0001.0101 of Integration Standard |

**Data Standard**

|  |  |
| --- | --- |
| **Reference Number** | 01.02.0001.0101 |
| **Service Invoking Fields** | |
| **Mandatory Fields**    1. User Name in English  2. Password in Bangla | **Optional Fields** |
| **Service Response Fields** | |
| 1. Status 2. JwtToken | |

**Fields Details**

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Field Type** | **Detail description** |
| Name in English | Varchar | This field will hold the name of a Person in English. Only Character are allowed for a name .No number or special character are allowed for a name. |
| Password in English | Varchar | This field will hold the password of the corresponding user. |
| Status | Varchar | This field indicates the success or failure of the login process. |
| JwtToken | Varchar | This filed contains all the information of the user including ( username,employee\_record\_id,office\_id,designation,office\_unit\_id,incharge\_label,office\_unit\_organogram\_id,office\_name\_eng,office\_name\_bng,office\_ministry\_id,office\_ministry\_name\_eng,office\_ministry\_name\_bng,unit\_name\_eng,unit\_name\_bng ) as encoded form. |

**Integration Standard**

|  |  |
| --- | --- |
| Reference No | 01.02.0001.0101 |
| Invoking Uri | doptor.gov.bd/loginWithIdp |
| Example of request | Request Uri- doptor.gov.bd/IdentityServer/ssologin?appName=oisf  Request Body:  {  username: superman  password:12345  } |
| Service Response | Response code : 200 interpretation : Successful Return.  Response code : 301 interpretation : Moved Permanently/Redirect.  Response code : 400 interpretation : Bad Request(Required info not present).  Response code : 401 interpretation : Unauthorized.  Response code : 403 interpretation : Forbidden.  Response code : 404 interpretation : Not Found.  Response code : 405 interpretation : Request method not allowed.  Response code : 406 interpretation : Not Acceptable.  Response code : 408 interpretation : Request time out.  Response code : 500 interpretation : Internal Server Error. |
| Example of Response | Response Body: (on success)  {  Response :  {  Status: “success”  jwtToken : eyJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6InN1cGVybWFuIiwiZW1wbG95ZWVfcmVjb3JkX2lkIjowLCJvZmZpY2VfaWQiOjUzLCJkZXNpZ25hdGlvbiI6IlN1cGVyTWFuIiwib2ZmaWNlX3VuaXRfaWQiOjUzLCJpbmNoYXJnZV9sYWJlbCI6MCwib2ZmaWNlX3VuaXRfb3JnYW5vZ3JhbV9pZCI6MSwib2ZmaWNlX25hbWVfZW5nIjoi  TWluaXN0cnkgb2YgUHVibGljIEFkbWluaXN0cmF0aW9uIiwib2ZmaWNlX25hbWVfYm5nIjoi4Kac4Kao4Kaq4KeN4Kaw4Ka24Ka-4Ka44KaoIOCmruCmqOCnjeCmpOCnjeCmsOCmo-CmvuCmsuCnnyIsIm9mZmljZV9taW5pc3RyeV9pZCI6NSwib2ZmaWNlX21pbmlzdHJ5X25hbWVfZW5nIjoiTWluaXN0cnkgb2YgUHVibGljIEFkbWluaXN0cmF0a  W9uIiwib2ZmaWNlX21pbmlzdHJ5X25hbWVfYm5nIjoi4Kac4Kao4Kaq4KeN4Kaw4Ka24Ka-4Ka44KaoIOCmruCmqOCnjeCmpOCnjeCmsOCmo-CmvuCmsuCnnyIsInVuaXRfbmFtZV9lbmciOiJEIDUiLCJ1bml0X25hbWVfYm5nIjoi4Kaq4Kaw4Ka\_4Kaa4Ka-4Kay4KaVIC0g4KerIn0.y3qgkdkFXN45NWkWcFQE\_qYyJOappx0sny2KYxgdZhE  [  The token contains following :  {  "username": "superman",  "employee\_record\_id": 0,  "office\_id": 53,  "designation": "SuperMan",  "office\_unit\_id": 53,  "incharge\_label": 0,  "office\_unit\_organogram\_id": 1,  "office\_name\_eng": "Ministry of Public Administration",  "office\_name\_bng": "জনপ্রশাসন মন্ত্রণালয়",  "office\_ministry\_id": 5,  "office\_ministry\_name\_eng": "Ministry of Public Administration",  "office\_ministry\_name\_bng": "জনপ্রশাসন মন্ত্রণালয়",  "unit\_name\_eng": "D 5",  "unit\_name\_bng": "পরিচালক - ৫"  }  ]  }  }  Response Body: (on failure) {  Response{  Status: “failure”  Reason: “Invalid Token”  }  } |
|  |  |

**Core Service Name: ‘ Wizard Login’**

**Service Metadata Definition**

|  |  |  |
| --- | --- | --- |
| **Serial No** | **Service Information** | **Description** |
| 1 | Reference Number | 01.01.0001.0102 |
| 2 | Service Name | Wizard Login |
| 3 | Description of Service | An user can login from one application to another application with wizard |
| 4 | Owner | OISF |
|  | Output type (Data/Service) | Service |
| 5 | Service Type ( Core/Shared) | Shared |
| 6 | Service Invoking Parameter | 1. From application id 2. To application id 3. User name 4. Expiry date 5. Company name 6. Authentication token |
| 7 | Mandatory Fields for service Invocation | 1. From application id 2. To application id 3. User name 4. Authentication token 5. Expiry date |
| 8 | Data Reference Model (DRM) | See 01.02.0001.0102 of Data Standard |
| 9 | Application Integration Reference Model (AIRM) | See 01.03.0001.0102 of Integration Standard |

**Data Standard**

|  |  |
| --- | --- |
| **Reference Number** | 01.02.0001.0102 |
| **Service Invoking Fields** | |
| **Mandatory Fields**     1. From application id 2. To application id 3. User name 4. Expiry date 5. Authentication token | **Optional Fields**    1. Company name |
| **Service Response Fields** | |
| 1. Status 2. Message | |

**Fields Details**

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Field Type** | **Detail description** |
| From application id | Varchar | An application which is requesting identity server to perform login for an user to another application. For example an user logs into oisf and want to login to grs. So here from application id = oisf |
| To application id | Varchar | The application to which an user wants to login with single sign on. For example an user logs into oisf now wants to sso to grs. Here to application id = grs. |
| Authentication token | Varchar | Jwt signed token which will contain necessary information.  1. Header  1.1 algorithm name  2. Payload will contain from  2.1 from application id,  2.2 to application id,  2.3 expiry date,  2.4 company name,  2.5 username.  3. Verify signature will be base64 url encoded hash value of the above.  Please find more details in <https://jwt.io/> |
| User name | Varchar | Unique user name who wants to perform single sign on. |
| Expiry Date | Varchar | Each token will have a validity period. After that it will be invalid. Time will be unix time in miliseconds. |
| Company name | Varchar | Name of the company for From application name |
| Status | varchar | This field indicates the success or failure of the login process. |
| Message | varchar | Detail Description of success or error in login process. |

**Integration Standard**

|  |  |
| --- | --- |
| Reference No | 01.03.0001.0102 |
| Invoking Uri | idp.doptor.gov.bd/wizardlogin |
| Example of request | Request Uri- idp.doptor.gov.bd/wizardlogin  Request Body:  {  fromApp : oisf  toApp : grs  userName : “bsaha”  expiryDate : “17/1/2018”  token : eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcm9tQXBwIjoib2lzZiIsInRvQXBwIjoiZ3JzIiwidXNlcm5hbWUiOiJoYXNzYW4iLCJleHBpcmVUaW1lIjoiMTIzNTY1ODc0NTYiLCJjb21wYW55TmFtZSI6IlJldmUgU3lzdGVtcyJ9.fx2lQVevKHj7Idak3R9G0D3j5tbjKzU3onIuvYMN08U  } |
| Service Response | Response code : 200 interpretation : Successful Return.  Response code : 301 interpretation : Moved Permanently/Redirect.  Response code : 400 interpretation : Bad Request(Required info not present).  Response code : 401 interpretation : Unauthorized.  Response code : 403 interpretation : Forbidden.  Response code : 404 interpretation : Not Found.  Response code : 405 interpretation : Request method not allowed.  Response code : 406 interpretation : Not Acceptable.  Response code : 408 interpretation : Request time out.  Response code : 500 interpretation : Internal Server Error. |
| Example of Response | Response (on success)  {  Status: “success”  Dashboard of the corresponding application  Msg: “”  }  Response Body: (on failure)  {  Status: “failure”  Login page with the following messages :  Msg:  {  1. Username or password not valid  2. Invalid app name  3. Invalid signature  }  } |

**Service Name: Dashboard Login**

**Service Metadata Definition**

|  |  |  |
| --- | --- | --- |
| **Serial No** | **Service Information** | **Description** |
| 1 | Reference Number | 01.01.0001.0103 |
| 2 | Service Name | Dashboard Login |
| 3 | Description of Service | An user can login from one application to another application with dashboard |
| 4 | Owner | Oisf |
|  | Output type (Data/Service) | Service |
| 5 | Service Type ( Core/Shared) | Shared |
| 6 | Service Invoking Parameter | 1. From application id 2. To application id 3. User name 4. Expiry date 5. Company name 6. Authentication token |
| 7 | Mandatory Fields for service Invocation | 1. From application id 2. To application id 3. User name 4. Authentication token 5. Expiry date |
| 8 | Data Reference Model (DRM) | See 01.02.0001.0103 of Data Standard |
| 9 | Application Integration Reference Model (AIRM) | See 01.03.0001.0103 of Integration Standard |

**Data Standard**

|  |  |
| --- | --- |
| **Reference Number** | 01.02.0001.0103 |
| **Service Invoking Fields** | |
| **Mandatory Fields**     1. From application id 2. To application id 3. User name 4. Expiry date 5. Authentication token | **Optional Fields**    1. Company name |
| **Service Response Fields** | |
| 1. Status 2. Message | |

**Fields Details**

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Field Type** | **Detail description** |
| From application id | Varchar | An application which is requesting identity server to perform login for an user to another application. For example an user logs into oisf and want to login to grs. So here from application name = oisf |
| To application id | Varchar | The application to which an user wants to login with single sign on. For example an user logs into oisf now wants to sso to grs. Here to application name = grs. |
| Authentication token | Varchar | Jwt signed token which will contain necessary information.  1.Header  1.1 algorithm name  2. Payload will contain from  2.1 application id,  2.2 to application id,  2.3 expiry date,  2.4 company name,  2.5 username.  3. Verify signature will base64 url encoded hash value of the above.  Please find more details in <https://jwt.io/> |
| User name | Varchar | Unique user name who wants to perform single sign on. |
| Expiry Date | Varchar | Each token will have a validity period. After that it will be invalid. Time will be unix time in miliseconds. |
| Company name | Varchar | Name of the company for From application name |
| Status | varchar | This field indicates the success or failure of the login process. |
| Message | varchar | Detail Description of success or error in login process. |

**Integration Standard**

|  |  |
| --- | --- |
| Reference No | 01.03.0001.0103 |
| Invoking Uri | idp.doptor.gov.bd/dashboardlogin |
| Example of request | Request Uri- idp.doptor.gov.bd/dashboardlogin  Request Body:  {  fromApp : oisf  toApp : grs  userName : “bsaha”  expiryDate : “17/1/2018”  token : eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcm9tQXBwIjoib2lzZiIsInRvQXBwIjoiZ3JzIiwidXNlcm5hbWUiOiJoYXNzYW4iLCJleHBpcmVUaW1lIjoiMTIzNTY1ODc0NTYiLCJjb21wYW55TmFtZSI6IlJldmUgU3lzdGVtcyJ9.fx2lQVevKHj7Idak3R9G0D3j5tbjKzU3onIuvYMN08U  } |
| Service Response | Response code : 200 interpretation : Successful Return.  Response code : 301 interpretation : Moved Permanently/Redirect.  Response code : 400 interpretation : Bad Request(Required info not present).  Response code : 401 interpretation : Unauthorized.  Response code : 403 interpretation : Forbidden.  Response code : 404 interpretation : Not Found.  Response code : 405 interpretation : Request method not allowed.  Response code : 406 interpretation : Not Acceptable.  Response code : 408 interpretation : Request time out.  Response code : 500 interpretation : Internal Server Error. |
| Example of Response | Response (on success)  {  Status: “success”  Dashboard of the corresponding application  Msg: “”  }  Response Body: (on failure)  {  Status: “failure”  Login page with the following messages :  Msg:  {  1. Username or password not valid  2. Invalid app name  3. Invalid signature  }  } |