NIE NATIONAL INSTITUTE OF EDUCATION SINGAPORE

An Institute of NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Federated Single Sign On (SSO)

--By

Eric Bonneau
S.Nedunchezhiyan

TRANSFORMING TEACHING
INSPIRING LEARNING

acis

Agenda

NIE-IAM Program

Federated Identity & SSO

NIE Identity Provider Setup

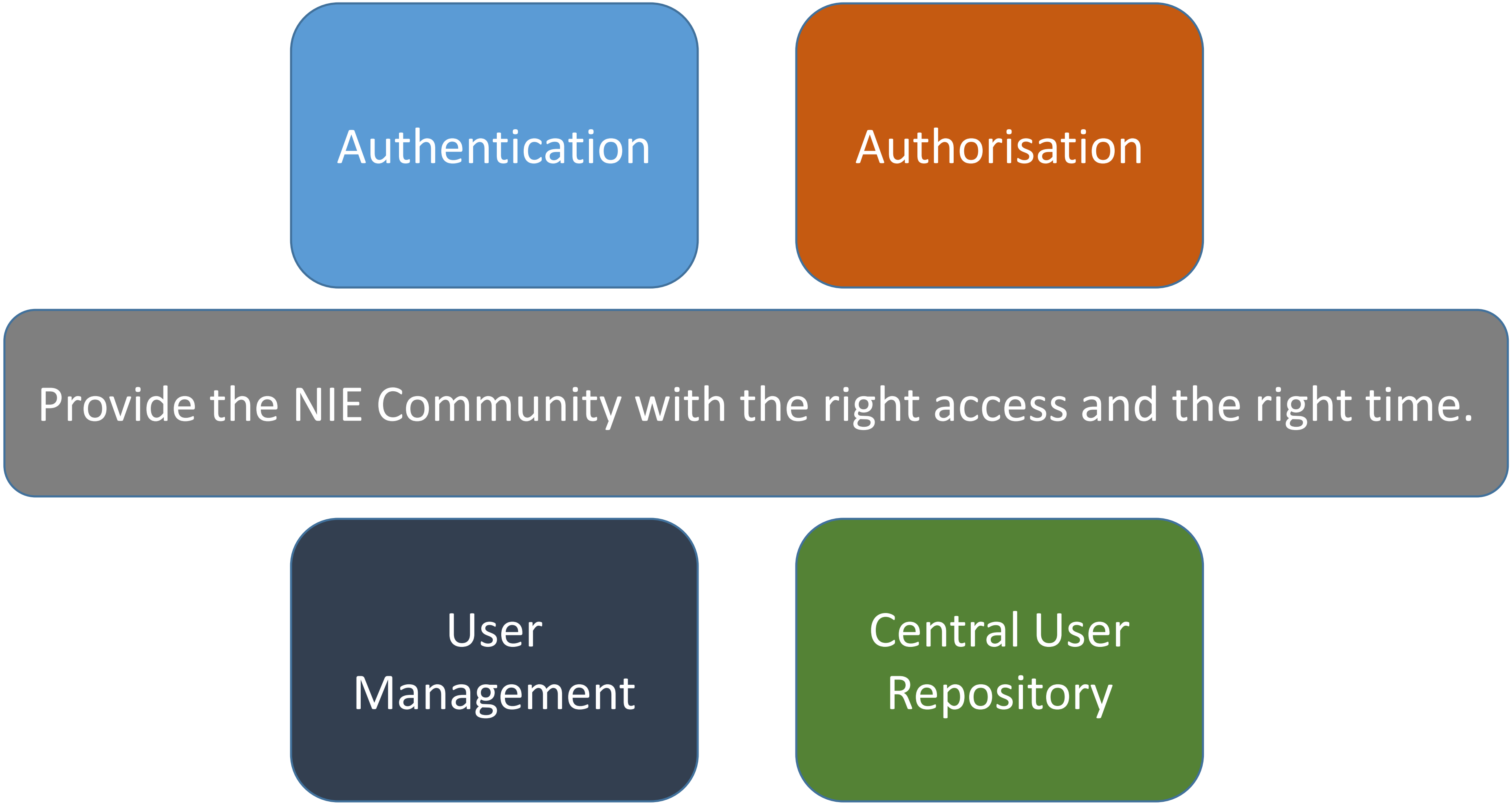
Federated-SSO Use Case

User Experience Demo

Benefits

Challenges

Identity and Access Management (IAM) program



Authentication

Authorisation

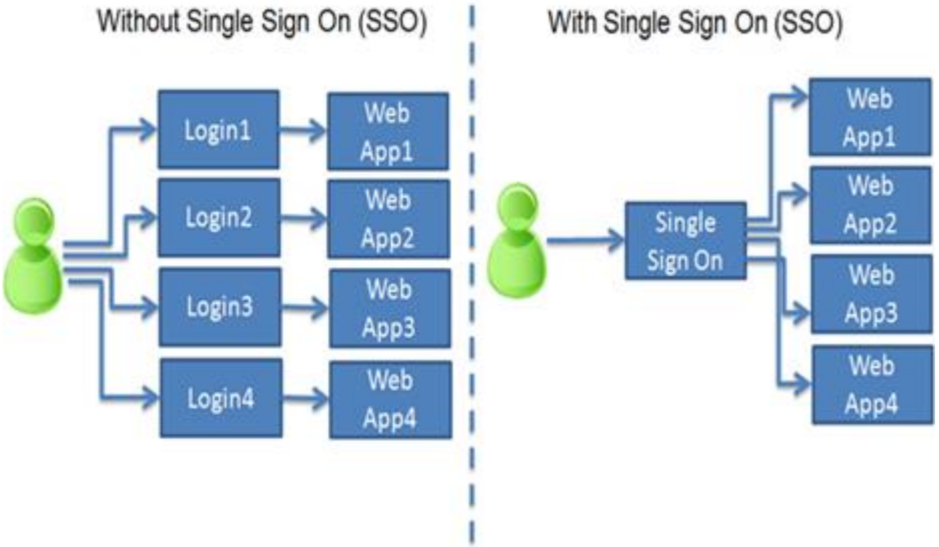
Provide the NIE Community with the right access and the right time.

User Management

Central User Repository

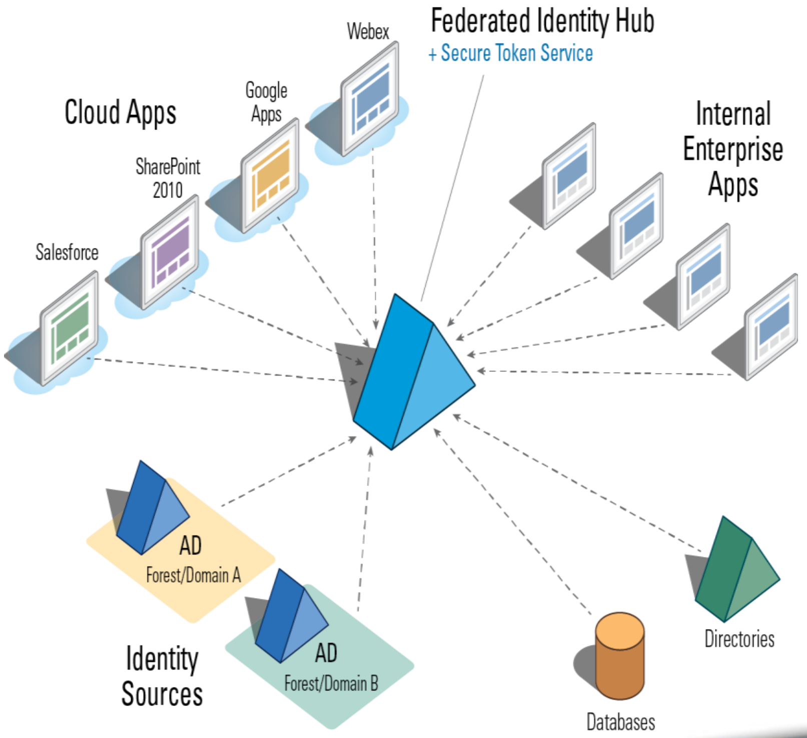
Single Sign-On (SSO)

Property that allows a user to access multiple systems with a single ID and password



Federated Identity

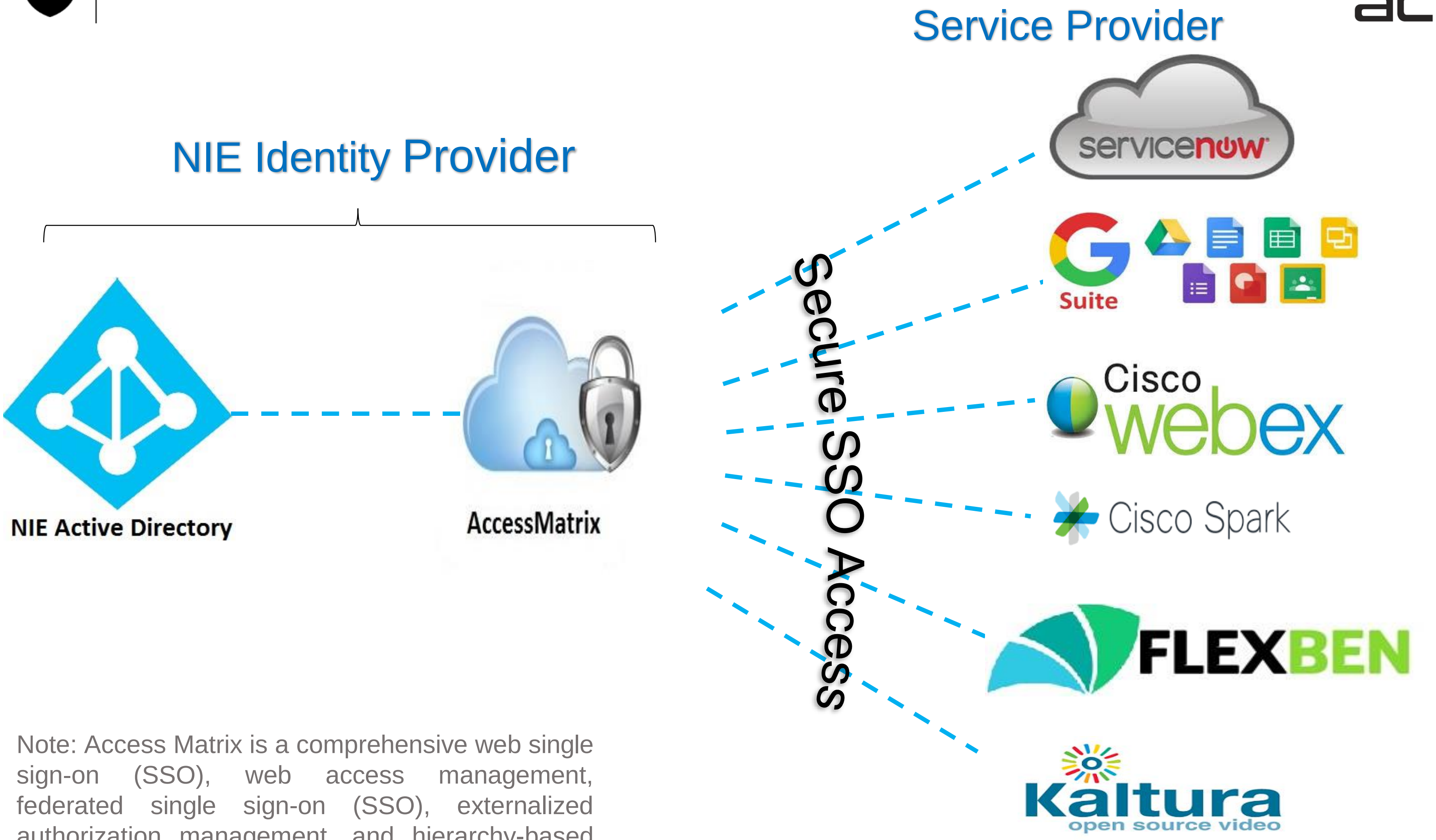
Federated identity is related to SSO as it links a user identity and attributes across multiple platforms



Cloud Application & SAML

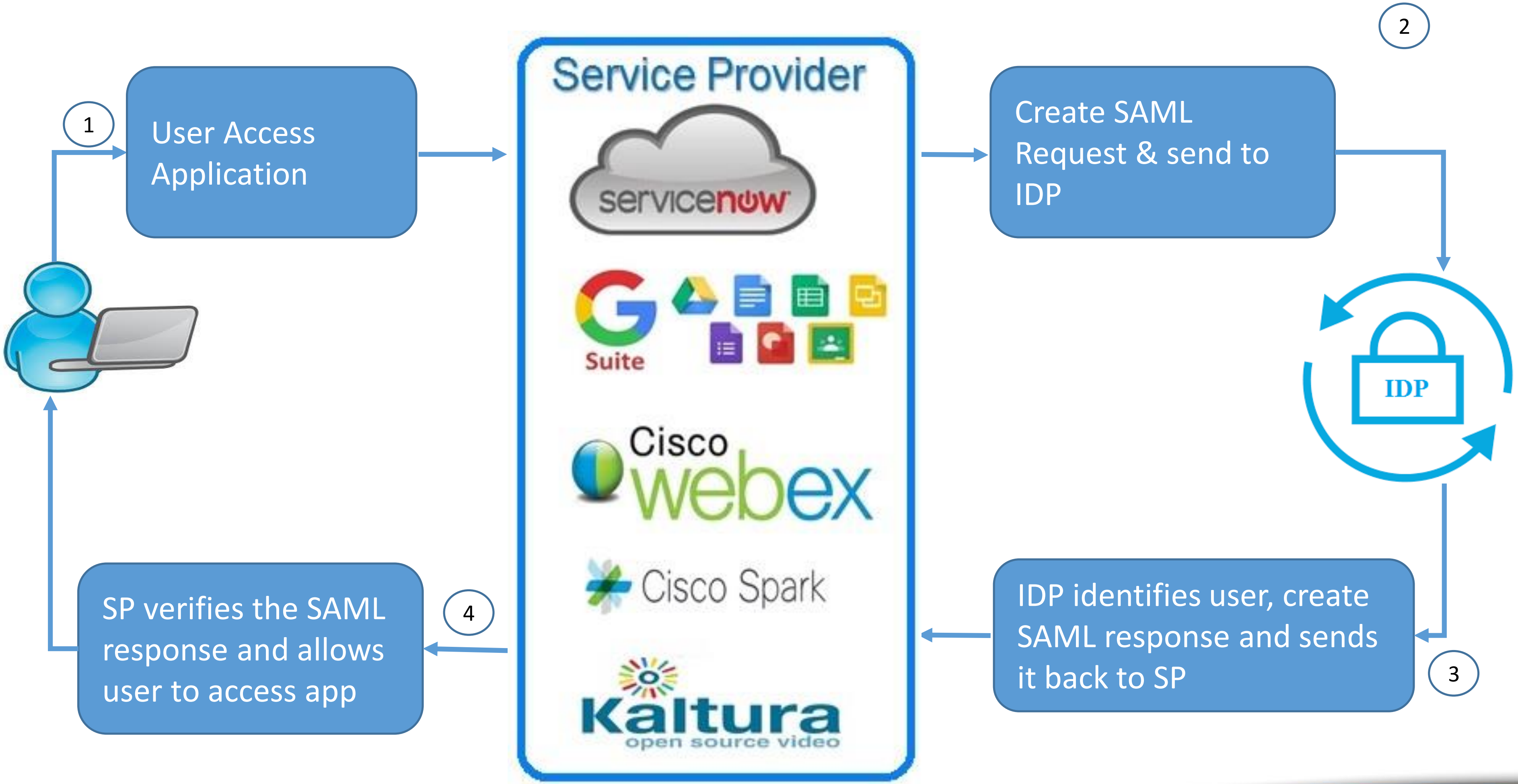
Cloud Application & SAML

NIE-IAM : NIE Identity and Access Management



Note: Access Matrix is a comprehensive web single sign-on (SSO), web access management, federated single sign-on (SSO), externalized authorization management, and hierarchy-based delegated administration system.

Federated Single Sign on – Use case



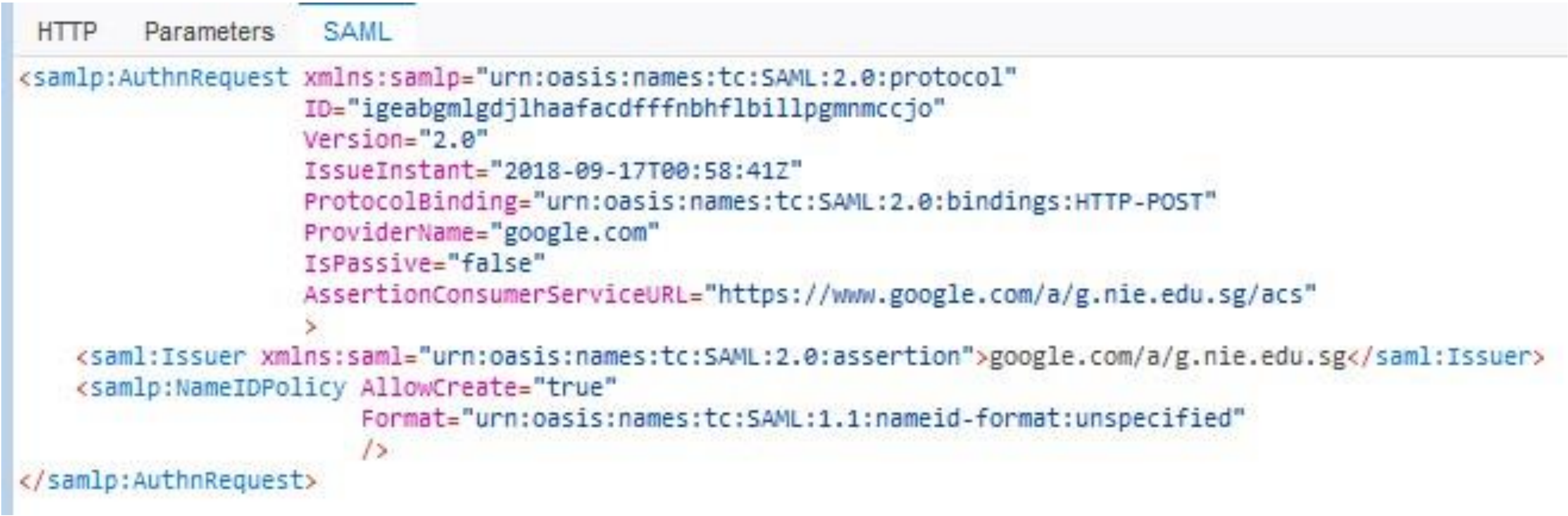
1 User Access Application

2 Create SAML Request & send to IDP

3 IDP identifies user, create SAML response and sends it back to SP

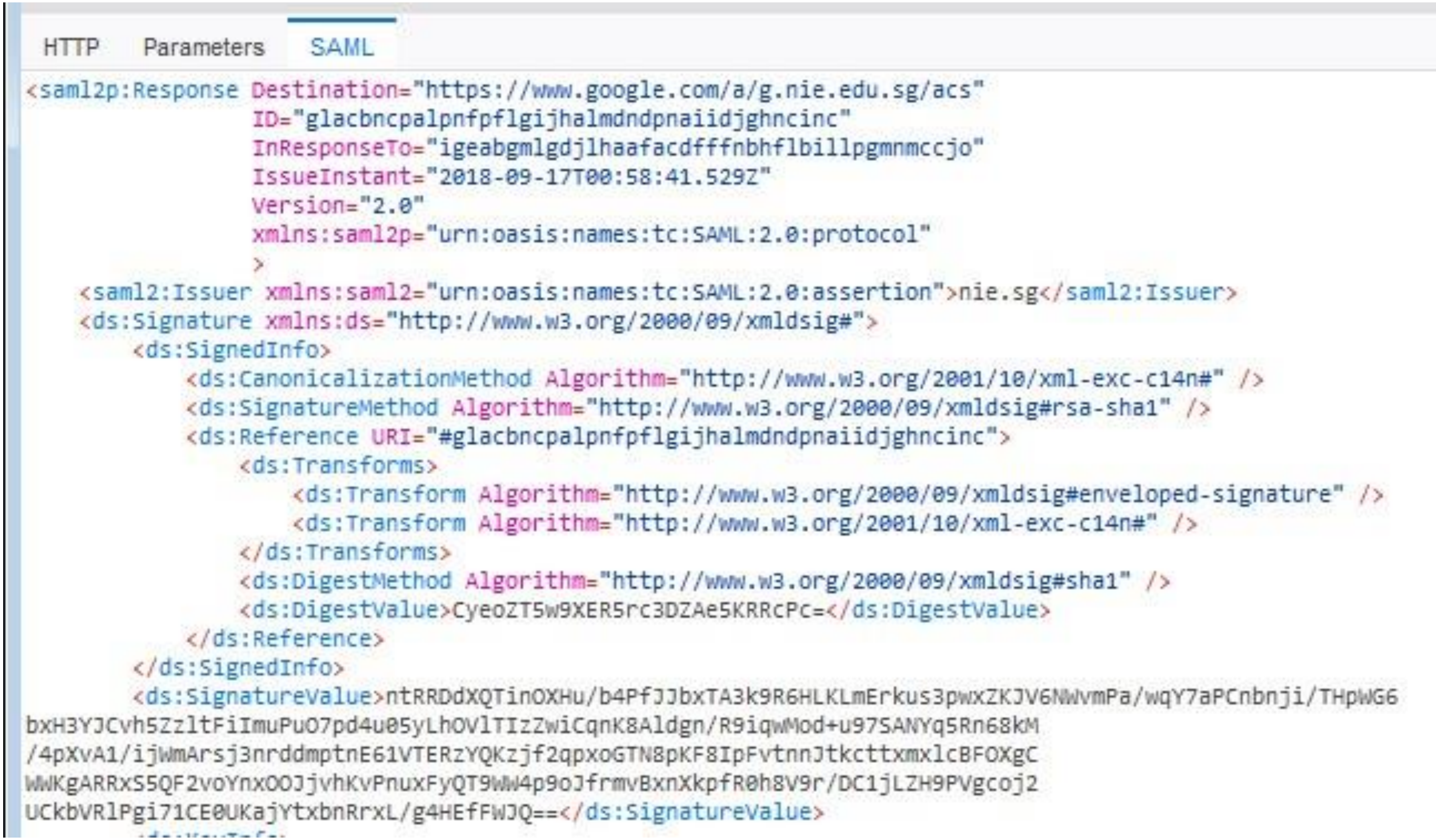
4 SP verifies the SAML response and allows user to access app

SAML Request Sample



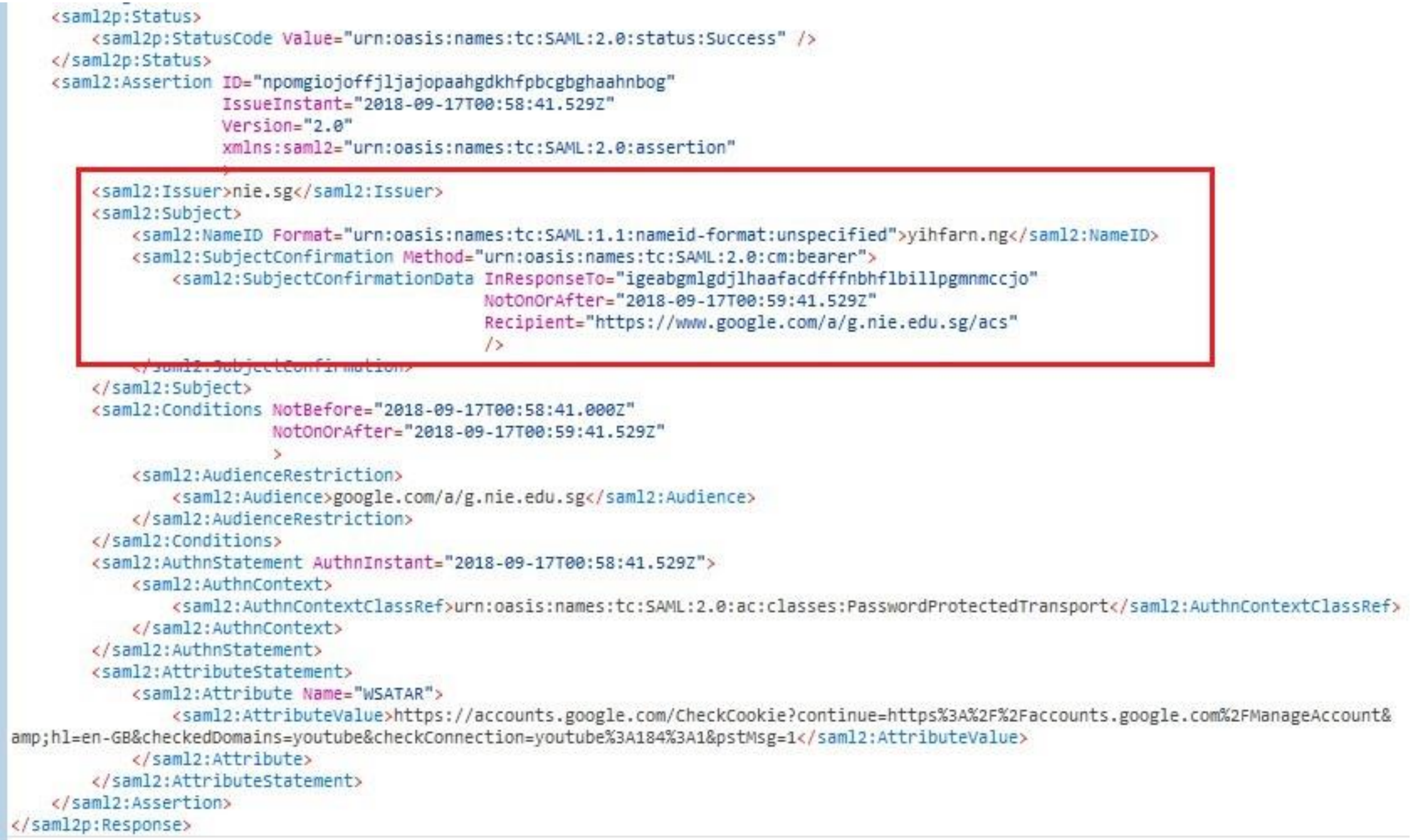
```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    ID="igeabgmlgdjlhaafacdfffnbhflbillpgmnmccjo"
                    Version="2.0"
                    IssueInstant="2018-09-17T00:58:41Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    ProviderName="google.com"
                    IsPassive="false"
                    AssertionConsumerServiceURL="https://www.google.com/a/g.nie.edu.sg/acs"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">google.com/a/g.nie.edu.sg</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="true"
                        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
                        />
</samlp:AuthnRequest>
```

SAML Response Sample



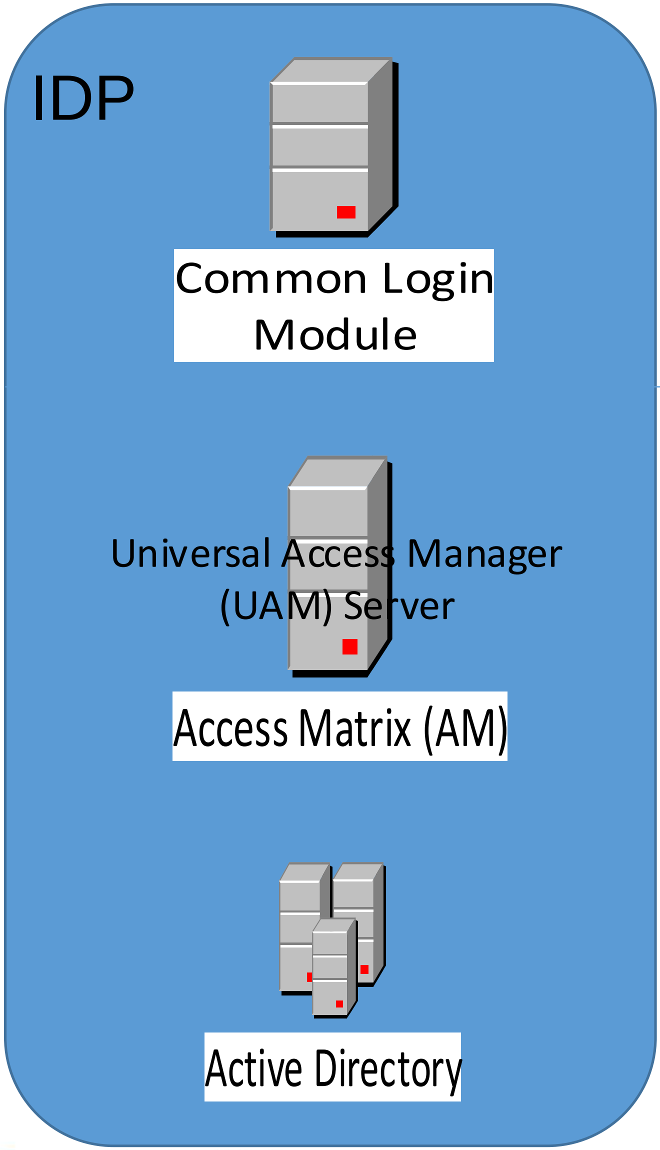
```
<saml2p:Response Destination="https://www.google.com/a/g.nie.edu.sg/acs"
                 ID="glacbncpalpnfpflgijhalmdndpnaiidjghncinc"
                 InResponseTo="igeabgmlgdjlhaafacdfffnbhflbillpgmnmccjo"
                 IssueInstant="2018-09-17T00:58:41.529Z"
                 Version="2.0"
                 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 >
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">nie.sg</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="#glacbncpalpnfpflgijhalmdndpnaiidjghncinc">
                <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>CyeoZT5w9XER5rc3DZAe5KRRcPc=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>ntRRDdXQTinOXHu/b4PfJJbxTA3k9R6HLKLmErkus3pwXZKJV6NWvmPa/wqY7aPCnbnji/THpWG6
bxH3YJCvh5Zzl tFiImuPuO7pd4u05yLhOVlTIzZwiCqnK8Aldgn/R9iqwMod+u97SANYq5Rn68kM
/4pXvA1/ijWmArsj3nrddmptnE61VTERzYQKzjf2qpxoGTN8pKF8IpFvtnnJtkcttxmxlcBFOXgC
WWKgARRxS5QF2voYnxOOJjvhKvPnuxFyQT9WW4p9oJfrmvBxnXkpfR0h8V9r/DC1jLZH9PVgcoj2
UCkbVRlPgi71CE0UKajYtxbnRrxL/g4HEfFWJQ==</ds:SignatureValue>
```

SAML Response Sample



```
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion ID="npomgiojoffjljajopaahgdkhfpbcgbghaahnbog"
                     IssueInstant="2018-09-17T00:58:41.529Z"
                     Version="2.0"
                     xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                     >
        <saml2:Issuer>nie.sg</saml2:Issuer>
        <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">yihfarn.ng</saml2:NameID>
            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml2:SubjectConfirmationData InResponseTo="igeabgmlgdjlhaafacdfffnbhflbillpgmnmccjo"
                                               NotOnOrAfter="2018-09-17T00:59:41.529Z"
                                               Recipient="https://www.google.com/a/g.nie.edu.sg/acs"
                                               />
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions NotBefore="2018-09-17T00:58:41.000Z"
                          NotOnOrAfter="2018-09-17T00:59:41.529Z"
                          >
            <saml2:AudienceRestriction>
                <saml2:Audience>google.com/a/g.nie.edu.sg</saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2018-09-17T00:58:41.529Z">
            <saml2:AuthnContext>
                <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
            <saml2:Attribute Name="WSATAR">
                <saml2:AttributeValue>https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Faccounts.google.com%2FManageAccount&
amp;hl=en-GB&checkedDomains=youtube&checkConnection=youtube%3A184%3A1&pstMsg=1</saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

NIE Identity Provider Components

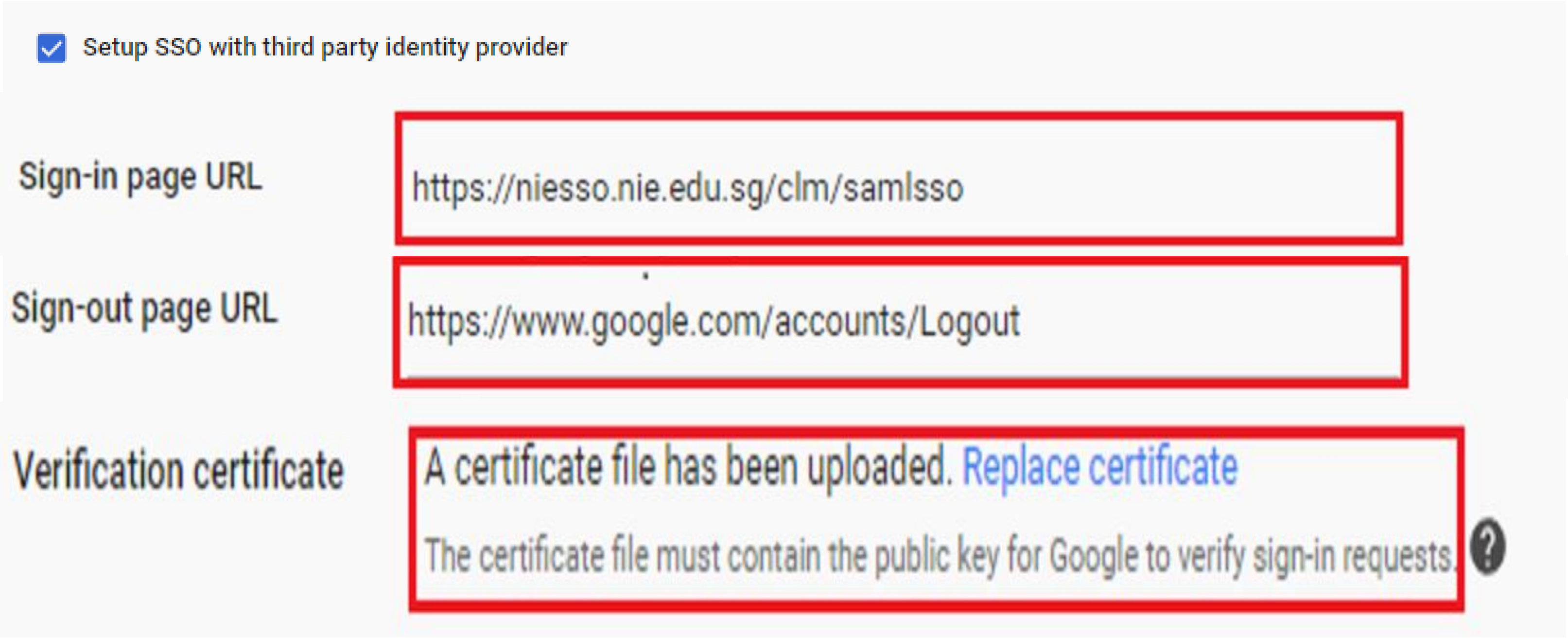


Common Login Module (CLM) is the User Facing IDP Front End. It hosts Login, Logout, Redirection Page.

UAM Server is the IDP Back End which performs Authentication, SAML Request Verification and SAML Response generation.

LDAP directory which stores the user credentials

Service Provider (SP) Configuration



☑ Setup SSO with third party identity provider

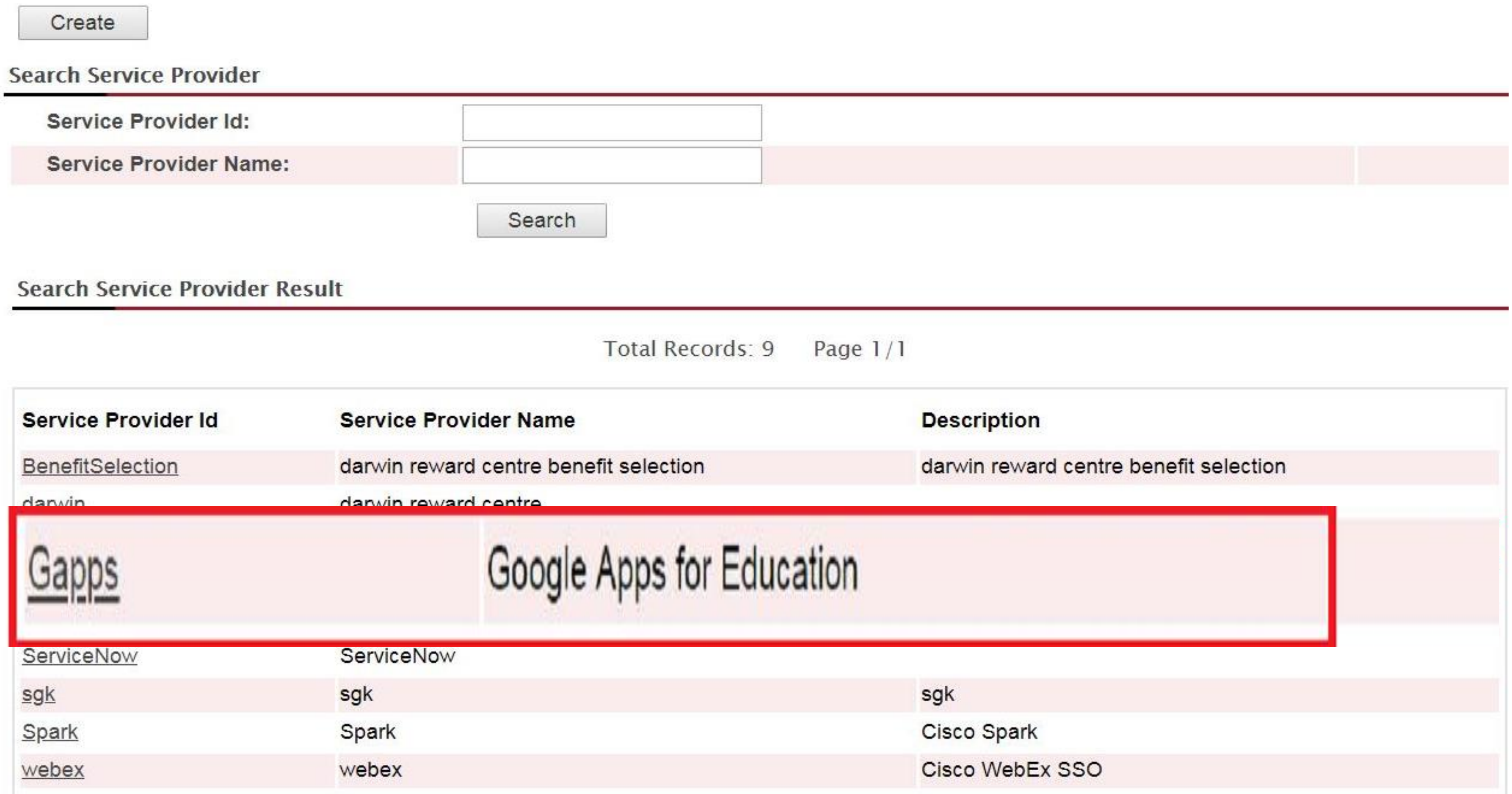
Sign-in page URL https://niesso.nie.edu.sg/clm/samlsso

Sign-out page URL https://www.google.com/accounts/Logout

Verification certificate A certificate file has been uploaded. Replace certificate

The certificate file must contain the public key for Google to verify sign-in requests.

Identity Provider (IDP) Configuration



Create

Search Service Provider

Service Provider Id:	
Service Provider Name:	

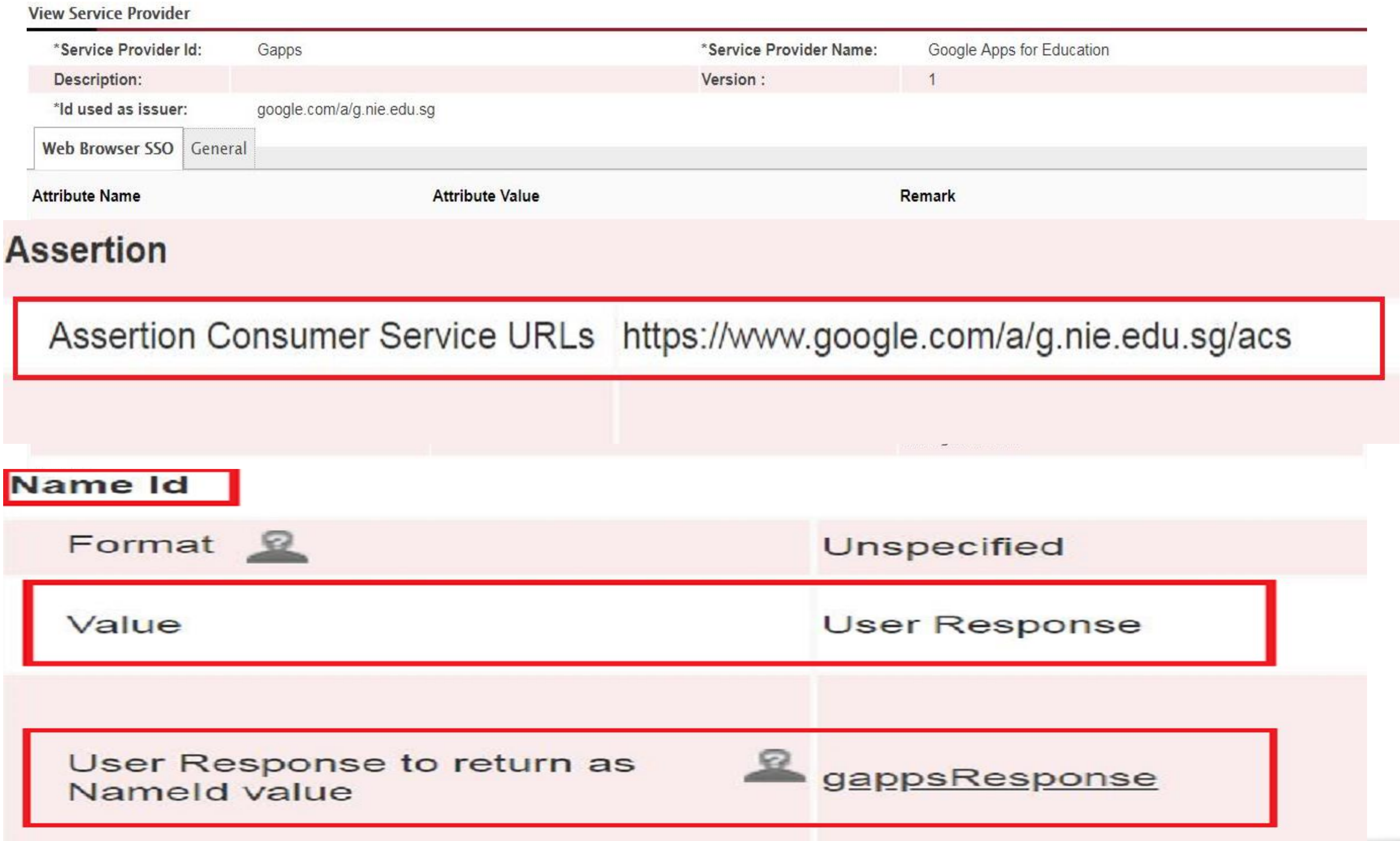
Search

Search Service Provider Result

Total Records: 9 Page 1/1

Service Provider Id	Service Provider Name	Description
BenefitSelection	darwin reward centre benefit selection	darwin reward centre benefit selection
darwin	darwin reward centre	
Gapps	Google Apps for Education	
ServiceNow	ServiceNow	
sgk	sgk	sgk
Spark	Spark	Cisco Spark
webex	webex	Cisco WebEx SSO

Identity Provider (IDP) Configuration



View Service Provider

*Service Provider Id:	Gapps	*Service Provider Name:	Google Apps for Education
Description:		Version :	1
*Id used as issuer:	google.com/a/g.nie.edu.sg		

Attribute Name	Attribute Value	Remark

Assertion

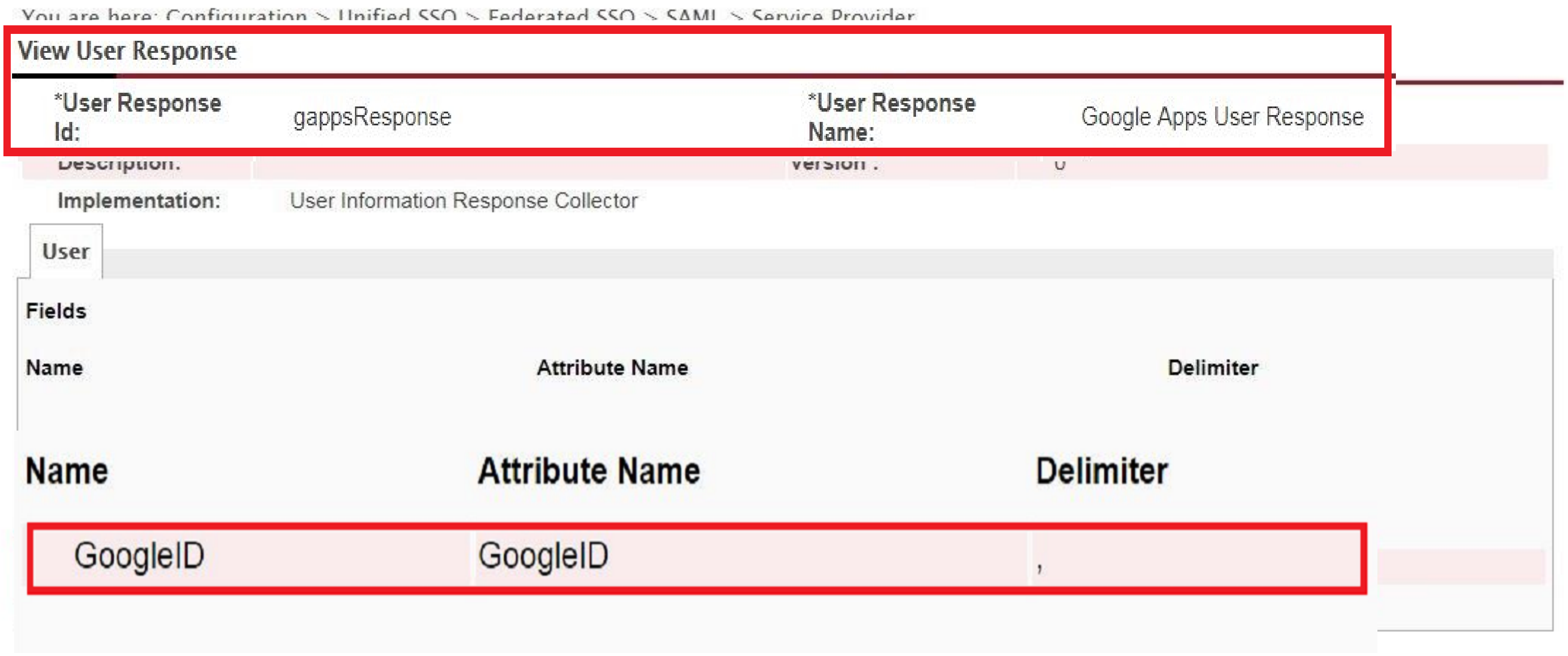
Assertion Consumer Service URLs	https://www.google.com/a/g.nie.edu.sg/acs

Name Id

Format	Unspecified
Value	User Response
User Response to return as NameId value	gappsResponse

Identity Provider (IDP) Configuration

User Response to return as NameId value (gappsResponse)



You are here: Configuration > Unified SSO > Federated SSO > SAML > Service Provider

View User Response

*User Response Id:	gappsResponse	*User Response Name:	Google Apps User Response
Description:		Version :	0
Implementation:	User Information Response Collector		

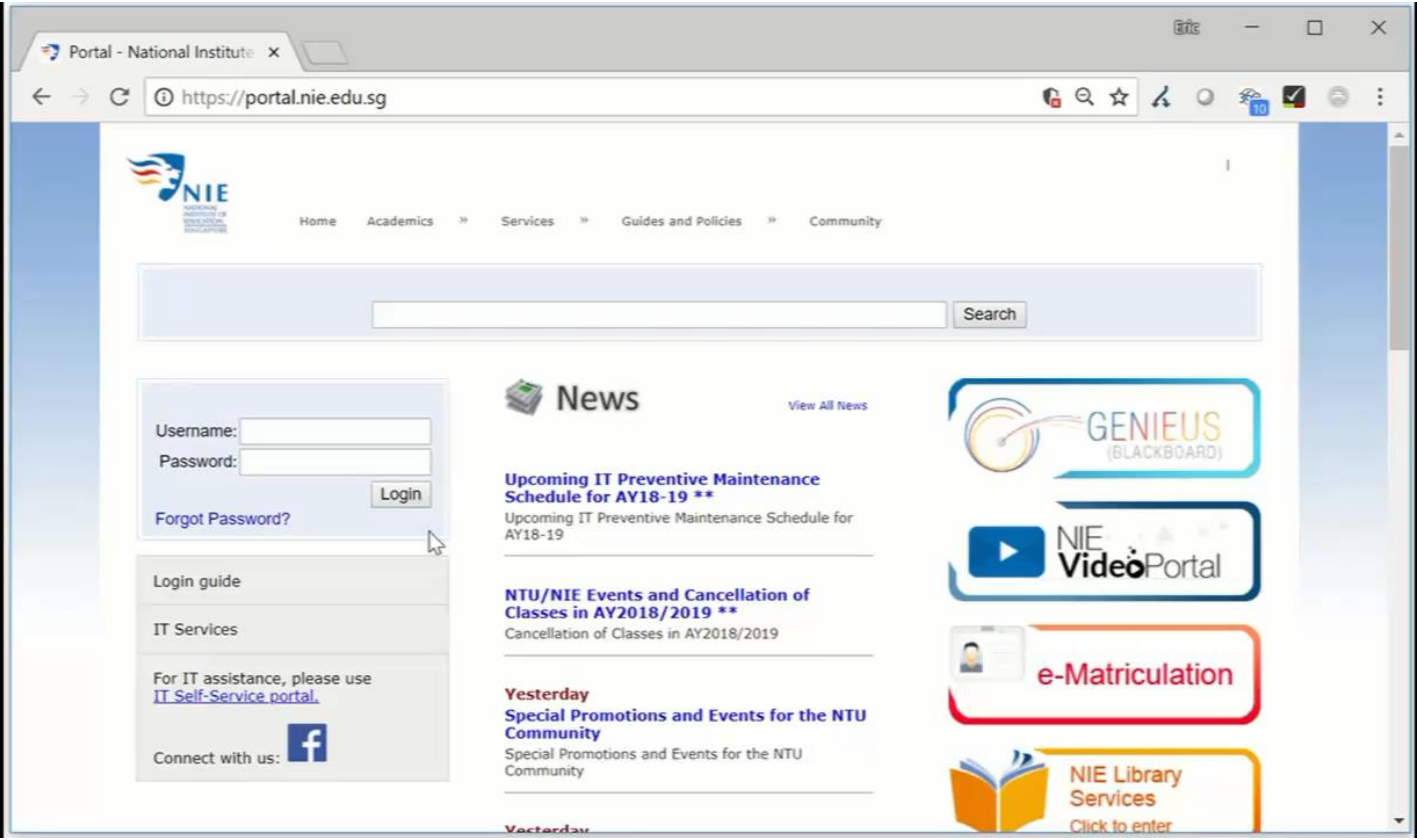
Fields

Name **Attribute Name** **Delimiter**

Name	Attribute Name	Delimiter
GoogleID	GoogleID	,

User Experience Demo

User Experience Demo



Portal - National Institute

https://portal.nie.edu.sg

Home Academics » Services » Guides and Policies » Community

Search

Username:

Password:

Login

Forgot Password?

Login guide

IT Services

For IT assistance, please use [IT Self-Service portal.](#)

Connect with us:

News

View All News

Upcoming IT Preventive Maintenance Schedule for AY18-19 **

Upcoming IT Preventive Maintenance Schedule for AY18-19

NTU/NIE Events and Cancellation of Classes in AY2018/2019 **

Cancellation of Classes in AY2018/2019

Yesterday

Special Promotions and Events for the NTU Community

Special Promotions and Events for the NTU Community

Yesterday

GENIEUS (BLACKBOARD)

NIE VideoPortal

e-Matriculation

NIE Library Services

Click to enter

Benefits

1. **Single Identity**: Users just remember single username & password to access different types of applications like Enterprise/Cloud/Mobile.

2. **Reduced Security Risks:** With Federated Identity, you can keep the authentication process within your on-premises Active Directory, enabling increased security. Using this model, you don’t have to synchronize password across different service providers.

3. **Increased Productivity:**

   For Users : The users have only one set of credentials to manage.

   For IT departments : Centralizing access control means one place to manage and monitor app access. Less calls to the helpdesk regarding user management.

   For Service Providers : They can securely and conveniently do business with your organization

Challenges

1. Working with some service provider is challenging, because in some cases they are not familiar with the concept related to Federated SSO.

2. Different requirement from different service provider.

3. Testing/Staging setup is not possible for all service providers.

4. Troubleshooting and coordination with Service Providers.

Q
&
A

Contact Us

Name	Email	Office Phone
BONNEAU Eric	eric.bonneau@nie.edu.sg	67903049
S.Nedunchezhiyan	nedunchezhiyan.s@nie.edu.sg	67903054

acis

Thank you