Singpass / CorpPass Project

Phase 2 Design

CorpPass Authentication and Authorization Interface Specification

accenture

SingPass / CorpPass Project

CorpPass Interface Specification

DOCUMENT INFORMATION

Business Focus Group / Agency	GovTech
Document Title	SPCP Phase 2 – CorpPass Interface Specification
Status	In-Progress
Business Owner	GovTech
Reference Documents	
..	

SingPass / CorpPass Project

CorpPass Interface Specification

VERSION CONTROL

Prepared by:	Aditya Jayanthi
Date:	27 Feb 2014
Reviewed by:	GovTech
Date:	
Approved by:	GovTech
Date:	

Version History

Date	Version	Author	Description
28-10-2014	0.1	Aditya Jayanthi	Initial Draft
07-11-2014	0.2	Aditya Jayanthi	Updated draft. Ready for GovTech review
21-11-2014	0.3	Aditya Jayanthi	Updated Authorization XML/XSD based on feedback from SPCP Functional and GovTech teams. Draft ready for final GovTech review and approval.
23-11-2014	1.0	Aditya Jayanthi	Baselined version. Ready for release.
27-02-2015	1.1	Aditya Jayanthi	Updated version. Removed Attribute Query reference.
13-04-2015	1.2	Aditya Jayanthi	Updated the Login Redirect URL to include additional URL Parameters and URL Encoding
30-11-2015	1.3	Aditya Jayanthi	Updated the details of encryption algorithms used for assertion encryption and provided sample encrypted assertion for reference (Section 7.4) Updated Authorization XML structure for third party authorizations and clarified the format of XML is Assertion Attributes (Section 8.1) Updated Out-of-band connection requirement for CorpPass to support Internet OOB only (Section 5.5) Updated the details of information exchanged during Federated Authentication Flow (Section 4.4.2)

Date	Version	Author	Description
11-01-2016	1.3	Aditya Jayanthi	Updated possible values for CP Entity Status in Authorization XML Updated Authorization XML to include Start Date and End Date for each role assigned to the user. Updated XML field descriptions with descriptions for data type, field length and mandatory columns.
01-04-2016	1.3.1	Houston Toh / Roger Goh	Updated Transport Channel in Artifact Binding Authentication Message Flow under section 4.4.1. Removed the SSL certificates from the list of required certificates under section 5.3.
08-04-2016	1.3.2	Houston Toh / Roger Goh	Updated authorisation XSD schema.

31-05-2016	1.4	Vishal Boyro	Updates on sections below: • **Section 4.4.3.1** o New section for user info XML o Removed CPID tag o Updated description for CPUID tag o Added CPSystemUID tag o Added CPNonUEN_RegNo tag o Added CPNonUEN_Country tag o Added CPNonUEN_Name tag • **Section 4.4.3.2** o Updated section to remove use info from authorisation XML o Updated error value to be returned when no value is assigned to a mandatory parameter • **Section 4.4.3.3** o Updated section to remove use info from 3rd party authorisation XML, leaving 3rd party entity specific info o Updated error value to be returned when no value is assigned to a mandatory parameter • **Section 8.1.1:** o New section for user info XSD and XML o Updated Example CorpPass User Info XML – Base64 Encoded o Updated Example CorpPass User Info XML – Decoded • **Section 8.1.2:** o Removed user info from XSD and XML o Updated XSD, sample XML including base64 format • **Section 8.1.3:** o Removed user info from XSD and XML o Updated XSD, sample XML including base64 format • **Section 9.2 in Annexure C:** o Added the user 'cancel' scenario o Updated section 4.4.1 to include the user 'cancel' scenario. • **Section 10 – Annexure D:**

Date	Version	Author	Description
			○ Added 2FA attributes in the SAML Assertion- Section 10 – Annexure D on AuthnContext
31-05-2016	1.4.1	Roger Goh	Updates on sections below: • **Section 4.4.1, 9.2** ○ "Referer" URL is used instead of "Referral" URL. • **Section 4.4.3** ○ Removal of CorpPass User ID as an element in CorpPass XML (Same update as per 1.4 – Removed CPID tag)
23-01-2017	1.4.2	Roger Goh	Updates on sections below: • Replacement of the word 'e-Service' to 'Digital Service' throughout the document • **Section 4.4.1** ○ Updated on Step 7 and 8 of the Authentication Flow to supports TLS1.2 only. (Not TLS1.1 or higher). • **Section 4.4.3** ○ Updated <Subject> element contains 'System defined ID of the user' instead of user NRIC information. ○ Updated NRIC/FIN or Foreign ID of the user within the <UserInfo> element as "CPUID" attribute ○ Renamed the 'CP_TPEntID_SUB' attribute to 'CP_ClntEnt_SUB' attribute instead (to be in-sync with XSD found in Appendix 8.1.3) • **Section 7.3** ○ Updated NAMEID parameter contains 'System defined ID of the user'. ○ Updated <UserInfo> contains NRIC/FIN or Foreign ID as "CPUID" attribute • **Section 7.4** ○ Updated <Subject> element contains 'System defined ID of the user' (i.e. CP1234) • **Section 8.1.3** ○ Included the "Example CorpPass Third Party Authorization XML – Decoded"

14-06-2017	1.4.3	Roger Goh	Updates on sections below: • **Section 4.4.3** o Updated description, "The entity (UEN/non-UEN ID) that the user belongs to within the <AuthAccess> element" o Added description, "c. The third party relationship authorisation within the <TPAuthAccess> element." o Updated description "CorpPass assertion will always have one <AttributeStatement> element with <UserInfo> and <AuthAccess>" o Added description "Specific to Third-Party Authorization, <TPAuthAccess> XML would contain additional details of the authorization for the third-party user" • Added description to 4.4.3.1, please note that the <UserInfo> element is mandatory in all CorpPass SAML assertions." • Added description to 4.4.3.2, "please note that the <AuthAccess> element is mandatory in all CorpPass SAML assertions." • Added description to 4.4.3.3, "please note that the <TPAuthAccess> element is optional and is only added to existing <UserInfo> and <AuthAccess> elements for third-party scenario. • **Section 7.3** o Updated description (a) "<UserInfo> contains NRIC/FIN or Foreign ID as "CPUID" attribute, and <AuthAccess>" o Added description "(b) Specific to Third-Party Authorisation, the decrypted text would contain <TPAuthAccess> elements" • **Section 8.1.3** o Added description "Please note that this <TPAuthAccess> element will added to existing <UserInfo> and <AuthAccess> elements in the assertion for all Digital Services using

Date	Version	Author	Description
			CorpPass in third-party scenario ONLY."
21	1.5	Roger Goh	Updates on sections below: • Section 4.4.1 o Added text note on digital signature validation and certificate expiry in Step 7 and 8 on the "IdP Initiated, Artifact Binding Authentication Message Flow" table. • Section 4.4.2 & 10.1.4 o Two-factor Authentication (2FA) using CorpPass Soft Token – a new 2FA option for user via a CorpPass mobile application. • Section 8.1.1 o Add example for decoded Non-UEN User Info XML • Added Section 11 – Annexure E o The resultant XML for 9 different scenarios.

CONTENTS

1. INTRODUCTION

1.1 DOCUMENT SCOPE

The scope of this document is to provide the Interface Specifications for CorpPass authentication and authorization using SAML 2.0 as part of the SingPass/CorpPass (SPCP) project. Please note that this document explains the interface specifications for CorpPass authentication and authorization only. A separate Interface Specification document has been released for SingPass.

1.2 INTENDED AUDIENCE

The intended audiences for this document are the agency application responsible persons and the technical staff that will be implementing the integration of agency applications with CorpPass, such as enterprise architects, security analysts, and developers.

1.3 HOW TO READ THIS DOCUMENT?

This document is intended to provide the agencies with the details of SAML 2.0 implementation specific to SPCP project for CorpPass authentication and authorization. This is not meant to be a replacement for SAML specifications. Therefore, agencies are advised to read and understand the SAML 2.0 specifications before reading this document.

The major sections of this document are:

Section 2: Provides a high-level overview of CorpPass

Section 3: Provides an overview of Identity Federation

Section 4: Details the CorpPass Authentication and Authorization Interface specification that explains the profile, bindings, protocols and assertions used in SPCP project. It also details the login flow along with detailed sequence diagram and examples of messages exchanged in the flow.

Section 5: This section describes how agencies should integrate with Identity Provider (CorpPass). This section contains the worksheet for data that Service Providers (agencies) need to provide SPCP in order to establish the trust relationship between IdP and SP.

Section 6: This section provides a brief overview of the technology landscape of vendors, open source tools available for setting up Service Provider modules. **Please note that the list of technology vendors provided are for reference only. These vendors have neither been endorsed nor recommended by SPCP team for Service Provider Implementation.** It also lists the key capabilities required by agencies' Service Provider module for integration with CorpPass.

1.4 REFERENCE DOCUMENTS

The links below provide more details on SAML 2.0 specification and details around implementation of service provider module.

https://www.oasis-open.org/standards

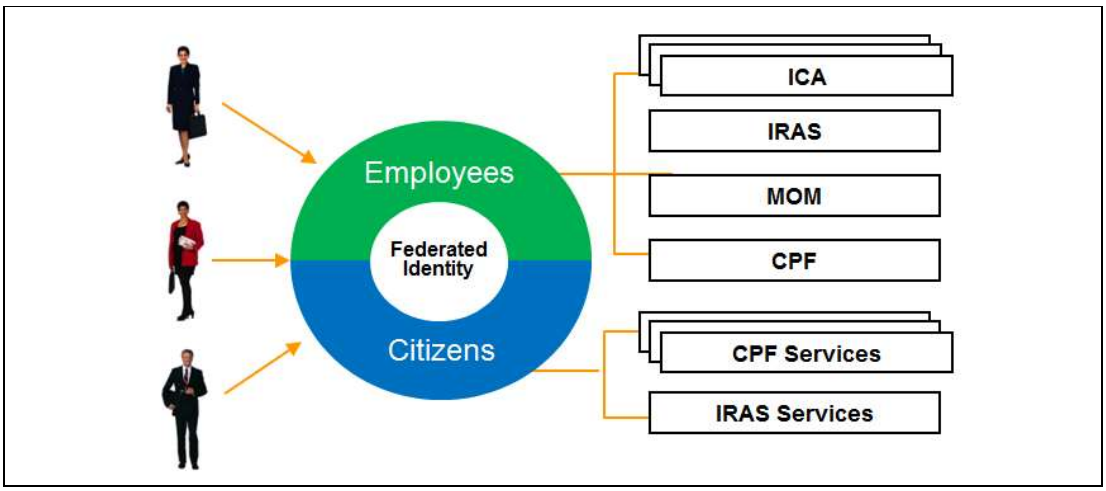
http://en.wikipedia.org/wiki/SAML-based_products_and_services

http://en.wikipedia.org/wiki/SAML_2.0

http://saml.xml.org/

https://wiki.oasis-open.org/security/FrontPage

2. WHAT IS CORPPASS?



CorpPass uses an identity federation infrastructure based upon IBM Tivoli Federated Management. We use this federation infrastructure to support the following primary use cases:

1. Authentication to internally/externally hosted web resources using CorpPass credentials

With CorpPass, users can enjoy the following benefits:

1. A shared trust model were user credentials who is known in one domain can be seamlessly introduced to another domain and vice-versa
2. Provides simplified sign-on to users and Improves user experience by delivering transparent access
3. Reduces administrative overhead of managing user identities

There are 2 main components in identity federation which are identity provider and service provider. CorpPass system serves as identity provider which gives assurances of the identity of the user to the other party. While agency will serve as service provider which trust the identity pass by CorpPass and allow the authenticated user to perform transaction in agency website.

3. WHAT IS FEDERATION?

3.1 IDENTITY FEDERATION

Identity federation is an arrangement made among multiple parties (such as government agencies) that lets users of the applications to use the same identification data to obtain access to multiple applications across agencies. E.g. Users can use their CorpPass credentials to access all agencies' Digital Services. The use of such a system is sometimes called Federated identity management (FIM).

Identity federation offers multiple advantages including

1. **Industrywide Standard**
   a. **Security Assertion Markup Language 2.0 (SAML 2.0)** is a SML based standard for exchanging authentication and authorization information between security domains.
   b. SAML 2.0 was ratified by **Organization for the Advancement of Structured Information Standards (OASIS)** and represents the convergence of SAML 1.1, Liberty ID-FF 1.2 and Shibboleth 1.3
2. **Interoperable**
   a. SAML is based on Service Oriented Architecture (SOA) which make it technology agnostic and can be implemented on any technology platform
3. **Extensive Support**
   a. SAML is a standard for implementing Federated Identity Management and there are a wide range of vendor products available to implement Federated Identity Management
   b. There are also open source options available for implementing Federated Identity Management that provide easy SAML 2.0 integration
4. **Standard Interface**
   a. The basic SAML exchange for federation is defined by the standard and any solution supporting the standard has to be compliant with the interface specifications. This means that agencies have access to standards based interface that will enable them to quickly implement solutions and with greater assurance

CorpPass utilizes federated identity management platform to provide user identification data to multiple agencies which agencies can utilize for providing access to users within their applications.

3.2 TRUST RELATIONSHIP

The key to federation is trusting that another party has done due diligence in verifying that identity. Trust relationship between an identity provider and a service provider allows a user to use a single federated identity and single sign-on when conducting business transactions with service providers. Each participant in a federated identity system must trust that the other participants are adhering to a set of practices that ensure the overall security is not compromised.

The technical aspects of trust management are generally implemented by exchanging cryptographic keys and other metadata that can be used to verify the identity of the parties. Well defined, broadly accepted policies and procedures must be in place, and independent assessment of these practices must be conducted to establish this trust.

External parties must be trusted to:

1. Vet identities before issuing credentials
2. Properly handle authentication of those identities
3. Provide identity and role information at time of access
4. Maintain the integrity of identity information throughout their system
5. Revoke identities properly
6. Input building trust

Elements of building trust include:

1. Legal Infrastructure
2. Audit and Accreditation
3. Shared Policy
4. Assertions
5. Technical Assurance
6. Cryptographic key management

3.3 SERVICE ORIENTED ARCHITECTURE

Federated identity management uses SOA architecture which offers interoperability and ensures that diverse applications can consume the service. The key highlights of the architecture are:

1. Capability of understanding and operating with a variety of formats for representing identity
2. Capable of translating between different identities
3. Based on SOA principles itself to deliver a flexible, infrastructure-based solution de-coupled from application business logic
4. Constructed using open standards to provide maximum interoperability with the platforms and systems on which SOA solutions are constructed

3.4 IDENTITY ASSURANCE

Identity assurance is the ability for a party to determine, with some level of certainty that an electronic credential representing an entity (an end user) with which they interact actually belongs to that entity and can be trusted to effect a transaction.

In the case where the entity is a person, identity assurance is the level at which the credential being presented can be trusted to be a proxy for the individual to whom it was issued and not someone else.

Identity assurance specifically refers to the degree of certainty of an identity assertion made by an identity provider (CorpPass) while presenting an identity credential to the Relying Party (agency).

CorpPass provides Two-factor authentication which adds a second level of authentication to an account log-in. When user have to enter only username and one password, that's considered a single-factor authentication. 2FA requires the user to have additional verification and with CorpPass, user need to perform OTP verification. These two levels of authentication are represented as two levels of assurance and Replying Party (agency), for example, can choose to allow only users at higher level of assurance to access the service or can users at both levels of assurance to access the service depending upon their requirements.

In CorpPass, each agency will have a choice to mandate the use of 2FA for access to a Digital Service and if an agency chooses this option all users trying to access that Digital Service will be asked to login using both the factors and the Service Provider for that Digital Service will allow only users with higher level of assurance to access the Digital Service.

4. CorpPass SAML Interface Specification

4.1 Identity Provider

CorpPass is the identity provider and it is the “vouch for” party in an identity federation. That is, it gives assurances of the identity of the user to the other party. The identity provider is responsible for:

1. Managing users and their identities
2. Issuing credentials
3. Handling user administration
4. Authenticating the user
5. Vouching for the user's identity with the service provider

4.2 Service Provider

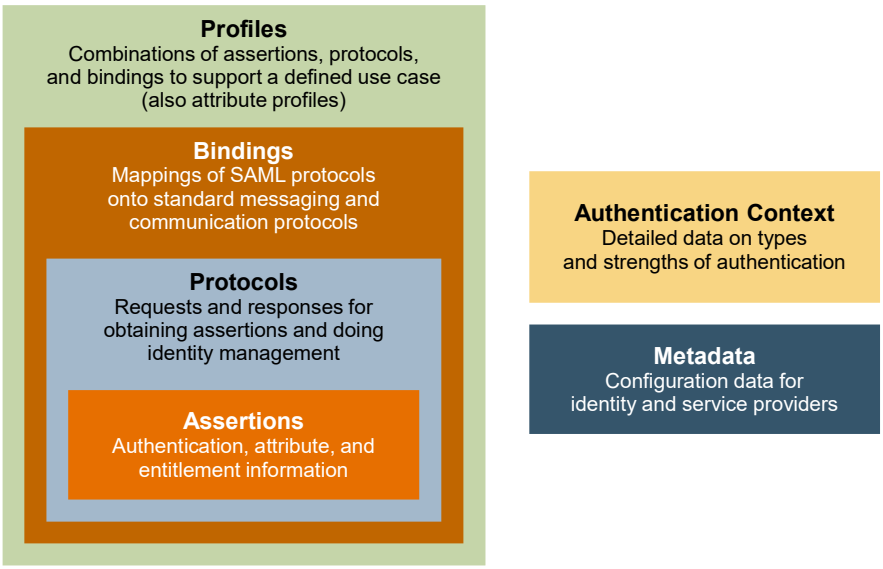
Agency will implement the service provider (sometimes called the relying party or resource partner or consumer) and the “validating party” in a transaction. The service provider is responsible for:

1. Controlling access to services
2. Validating the asserted identity information from the identity provider (typically by way of verifying a digital signature)
3. Providing access based on asserted identity
4. Managing only locally relevant user attributes, not an entire user profile

4.3 SAML Assertions, Protocols, Bindings and Profiles

The following diagram gives a high level view of SAML2.0. SAML 2.0 contains the following elements:

1. Assertions: Assertions contain the actual user data including their attributes (e.g. NRIC) and entitlements (e.g. roles, UEN etc.). Assertion details are pre-agreed between the CorpPass and agencies
2. Protocols: Protocols define the type of request that is being sent to the other party in the transaction i.e. When a SP wants to retrieve the user information from IdP after receiving the artifact, it sends an <ArtifactResolve> request to IdP as defined the Artifact Resolution protocol.
3. Bindings: Bindings refer to communication protocols used in exchanging of requests and assertions. CorpPass will use HTTP Artifact bindings
4. Profiles: Profile refers to a combination of bindings, protocols and assertions that together define how the federated identity data is exchanged. CorpPass will support Artifact Resolution profile
5. Authentication Context: Authentication Context provides the details of how a user has authenticated with IdP. This will allow the agencies to know if the user has used 1-factor or 2-factors when authenticating
6. Metadata: Metadata refers the data that is exchanged between Service Provider and Identity Provider while establishing the trust relationship. This will include the settings as well as crypto material.



4.3.1 Assertions

An assertion is a package of information that made by a SAML authority (Identity Provider). SAML assertions are usually made about a subject (user), represented by the <Subject> element. The SAML 2.0 specification defines three different kinds of assertion statements that can be created by a SAML authority. All SAML-defined statements are associated with a subject. In CorpPass we will be authenticating a user as well as provide authorization information about the user using the following statements:

1. Authentication Assertion: This assertion statement is issued during artifact resolution and provides the information regarding the assertion subject that includes tells that subject was authenticated by a particular means at a particular time. This statement will also contain the 2 attribute statements:
   a. <UserInfo> element, that provides the user identity information (Full Name, account status, User type, etc); and
   b. <AuthAccess> and/or <TPAuthAccess> element, that provides the authorization information regarding the subject which specifies the Entity (UEN/non-UEN ID), Digital Service and Role information of the user.

The following are the essential components of the SAML <Assertion> element:

1. a <saml:Issuer> element, which contains the unique identifier of the identity provider
2. a <ds:Signature> element, which contains an integrity-preserving digital signature over the <saml:Assertion> element
3. a <saml:Subject> element, which identifies the authenticated principal (user)
4. a <saml:Conditions> element, which gives the conditions under which the assertion is to be considered valid
5. a <saml:AuthnStatement> element, which describes the act of authentication at the identity provider. This also includes user's authentication context
6. a <saml:AttributeStatement> element, which provides the attribute information for the subject as requested by SP

Please refer to Annexure Section 7.1 for SAML 2.0 Assertion example.

Please note that Assertion will contain data in encrypted format where the user information in an assertion is encrypted. The complete list of tags in the <Assertion> element schema, the encryption algorithms used and the cryptographic material required for use in SAML messaging are listed in "Section 5.2 – Service Provider Configuration and Integration with IdP" below.

4.3.2 Protocols

Protocols define how the requests and responses are exchanged between Service Provider and Identity Provider. The steps below show the protocols used by CorpPass authentication and authorization:

1. User accesses agency's Digital Service login with CorpPass.
2. Agency's Service Provider module forwards the user to Identity Provider (CorpPass) with a return URL (to redirect back after authentication)
3. Identity Provider authenticates the user and sends the user back to Service Provider's return URL along with a SAML artifact
4. Service Provider initiates "Artifact Resolution Protocol <ArtifactResolve>" to request artifact resolution from Identity Provider
5. Identity Provider responds with "Artifact Response Protocol <ArtifactResponse> in which the Identity Provider sends the SAML Assertion with user authentication and authorization details to Service Provider

In the SAML exchange flow mentioned above, CorpPass uses the "Artifact Resolution" and "Artifact Response" protocols from the SAML specification. The following sections explain these protocols in more detail.

4.3.2.1 Artifact Resolution Protocol

The artifact resolution protocol provides a mechanism by which SAML protocol messages (assertions), can be transported in a SAML binding by reference instead of by value. Both requests and responses can be obtained by reference using this specialized protocol. A message sender (IdP), instead of binding a message to a transport protocol, sends a small piece of data called an artifact using the binding. An artifact provides a means by which the receiver (agency SP module) can determine who sent it i.e. if this is from IdP (CorpPass). Receiver can then use Artifact Resolution protocol in conjunction with SAML SOAP binding, sent over the back channel, to resolve the artifact into the original protocol message i.e. the SAML assertion with user details.

The objectives of using this protocol in CorpPass are

1. This protocol enables agencies to use the trusted back channel for retrieval of the user details which improves security
2. The normal bindings that are used over the browser cannot easily carry full message (i.e. the assertion) because of size constraints

The artifact sent to the agency service provider module using the binding uses a single-use semantic such that once it has been successfully resolved, it can no longer be used by any party. This means that it cannot be used by attacks such as replay attack to retrieve the assertions. The SAML SOAP

binding protocol used to resolve the artifact will require the use of mutual authentication i.e. server-to-server authentication to retrieve the assertion. This increases the overall security by ensuring that only trusted parties are able to retrieve the assertion which contains the user authentication and authorization details.

Regardless of the channel used for retrieving the assertion (which in our case is the out-of-band channel over intranet) the service provider must treat is as though it was originally retrieved in place of the artifact and treat the assertion as valid. The following elements outline the messages used during the retrieval of assertion over back channel.

1. Element <ArtifactResolve>: The <ArtifactResolve> message is used to request that a SAML protocol message be returned in an <ArtifactResponse> message by specifying an artifact that represents the SAML protocol message.
   a. The <ArtifactResolve> message should be signed by service provider to protect the integrity.
2. Element <ArtifactResponse>: When IdP receives the <ArtifactResolve> message it will respond with an <ArtifactResponse> message element. The <ArtifactResponse> message will be signed by IdP to protect the integrity.

4.3.3 Bindings

We are using Artifact Resolution profile along with Artifact Resolution Protocol for the back channel exchange of assertion information. As per SAML specification the binding used for this should be a synchronous binding and therefore CorpPass users SAML SOAP Binding (over HTTP) to resolve a SAML message.

4.3.4 Profiles

CorpPass uses Artifact Resolution profile with IdP Redirect Artifact flow. This login flow for this profile is explained in the ‘Section – IdP Initiated, Artifact Binding Authentication”.

4.3.5 Metadata

In order to establish a trusted relationship between Identity Provider and Service Provider for an agreed SAML profile, the parties must require agreements regarding identifiers, binding support and endpoints, certificates and keys, and so forth.

A metadata specification is useful for describing this information in a standardized way. This specification defines an extensible metadata format for SAML system entities, organized by roles that reflect SAML profiles, such as Identity Provider and Service Provider.

The metadata that needs to collected from Service Provider side (i.e. agencies) is listed “Section – Setting up Service Provider” below. The actual exchange of metadata will occur individually with each agency during transition phase.

4.3.6 Authentication Context

Agencies might require users to authenticate using different mechanisms based on the level of security required for a given Digital Service. In CorpPass solution there is an option for supporting second-factor authentication in addition to using the standard username and password (first-factor). Agencies can

choose the mandate the use of 2FA for selected Digital Services based on their requirements. The process for subscription to use 2FA is out-of-scope for this document and will be provided separately by the project.

When a user logs in with Identity provider which is the SAML authentication authority, it can deliver to the relying party (Service Provider) the additional authentication context information in the form of an authentication context declaration (using XML tags) inserted directly or referenced within the assertion that the identity provider sends to the service provider. Service Provider can then choose to read the authentication context in the assertion and base its decision to allow user to access resources on the level of authentication the user used while authenticating with IdP.

4.4 FEDERATED AUTHENTICATION FLOW

This section describes the flow and steps involved when a user accesses a Digital Service that is integrated with CorpPass using SAML 2.0 for federation.

4.4.1 IdP Initiated, Artifact Binding Authentication

What is IdP Initiated authentication?

CorpPass authentication used IdP initiated authentication using Artifact Resolution profile as per the SAML 2.0 specification.

IdP initiated refers the starting point of SAML exchange being the Identity Provider as opposed to Service Provider. SAML 2.0 provides option to either Service Provider or Identity Provider to initiate the authentication process. In CorpPass, when a user accesses the agency's Digital Service, the Digital Service redirects the user directly to Identity Provider URL, after which the Identity Provider initiates the process of authentication. Therefore, the profile we are using is called Identity Provider initiated authentication.

What is Artifact Binding?

Artifact binding refers to the way the user details are exchanged after the user is authenticated by the Identity Provider. As per SAML 2.0 specification, using this profile means that the Identity Provider cannot send the user details to SP using browser redirect but instead needs to send an artifact (used as reference) over browser redirection and instead use the back channel for actual user authentication and authorization details (assertion) exchange.

The following diagram shows how IdP initiated, Artifact Binding login flow works.

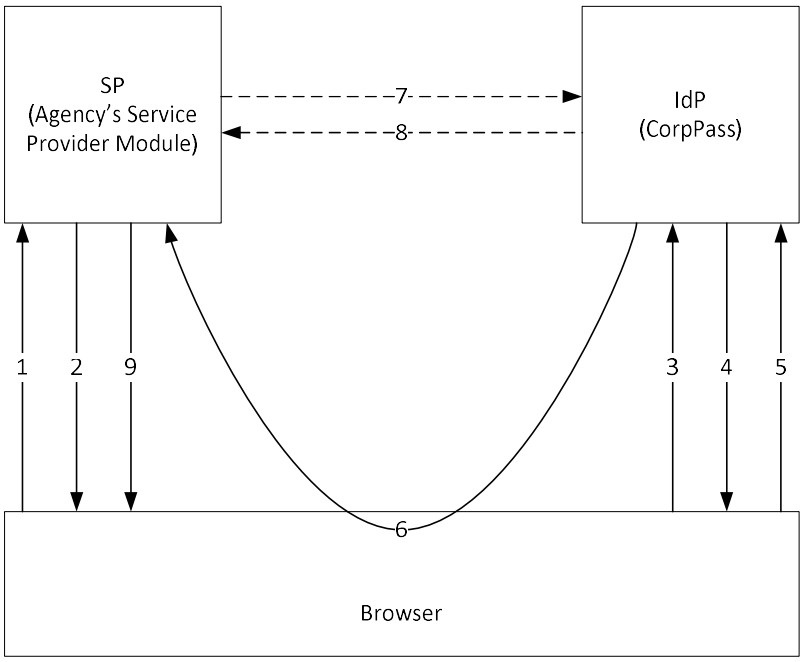


Figure – IdP Initiated, Artifact Binding Authentication Message Flow

The message flow for the new CorpPass based on SAML using IdP initiated Artifact Binding is as follows. Do note that additional internal system processing are intentionally removed to minimized confusion.

No.	Binding	Message Content	SAML Message (or Message Parts) Security	Transport Channel Security
1	HTTP	Public user makes requests for content not requiring authentication and the SP supplies non-sensitive content until sensitive (authenticated) content requested. Possibly cookie placed by the SP.	NA	NA
2	HTTP	Non-sensitive content are displayed. In addition, "Login to CorpPass"	NA	NA

No.	Binding	Message Content	SAML Message (or Message Parts) Security	Transport Channel Security
3	HTTP	Public user clicks on "Login to CorpPass" button. The button contains the trigger URL to SAML endpoints on IdP.	NA	TLS 1.0 or higher
4	HTTP	IdP presents logon page to public user's browser.	NA	TLS 1.0 or higher
5	HTTP	a) Public user logs on to IdP using their authentication key(s) (i.e. User ID and Password); or b) Public user 'click' on the 'Cancel' button.	NA	TLS 1.0 or higher
6	HTTPArtifact (carried in an HTTP Redirect)	a) If users performs step 5a, SAML Message: HTTP parameter carrying the dereference information (i.e. the SAML artifact) for the SAML Artifact Resolution protocol. b) If user performs step 5b, IdP would redirect the user back to Digital Service using 2 approaches: i. "Referer URL" if it's found in the HTTP request headers. ii. "Target" parameter if the "Referer URL" is not found. iii. In both cases (i & ii), a "errorcode=CorpPass_00_00_01" request parameter will be appended for the redirection. For more details please refer Section 9.2 in Annexure C on	• No XML Signature.No XML Encryption.	TLS 1.0 or higher

No.	Binding	Message Content	SAML Message (or Message Parts) Security	Transport Channel Security
		the format and values to be used.		
7	SOAP/HTTP Artifact (Artifact from Artifact Resolution profile)	SAML Message: SAML <ArtifactResolve> element.	• XML Signature must be used by Requesting Agency (SP). • No XML Encryption. **Note: CorpPass to validate Agency's digital signature with full trust-chain and SP's public certificate.** **Agency to inform SPCP project team when there is a certificate renewal.**	One-way TLSv1.2 through our WAF (Web Application Firewall) and the certificate presented will be WAF certificate.
8	SOAP/HTTP Artifact (Artifact from Artifact Resolution profile)	SAML Message: SAML <ArtifactResponse> element with the protocol message associated with the artifact; a SAML <Response> message in this case. The <Response> message contains the assertion with the details of the user's IC and entity/role information in the form of XML.	XML Signature must be used along with XML Encryption for assertion by CorpPass. **Note: CorpPass to validate Agency's digital signature with full trust-chain and SP's public certificate.** **Agency to inform SPCP project team when there is a certificate renewal.**	One-way TLSv1.2 through our WAF (Web Application Firewall) and the certificate presented will be WAF certificate.
9	HTTP Redirect	Public user accesses sensitive (authenticated) content requested. This is an internal step carried out within the agency between SP and Digital Service application. Possibly cookie placed by the SP.	NA	TLS 1.0 or higher (depending on Agencies' security policy)

Note: SSL v2 and SSL v3 has since been deprecated and will NOT be supported by CorpPass.

4.4.2 Information Exchanged during Federated Authentication Flow

This section provides a high-level overview of the attributes and details that are exchanged during the federated authentication flow. The aim of this section is to highlight the key attributes/information that agency needs to consider during CorpPass authentication. **Please note the defined Parameters and its value are case sensitive as defined in this specification,** please refer to Section 9.1 for more details in Annexure C.

Authentication Step	Parameters Sent (from SP to IdP)	Parameters Returned (from IdP to SP)
Authentication Redirection	• **RequestBinding** • **ResponseBinding** • **PartnerId** • **Target** • **NameIdFormat** • **esrvcID** For more details please refer to Section 9.1 in Annexure C on the format and values to be used.	• **SAML Artifact**: A random unique string that is to be exchanged using out-of-band channel to fetch assertion containing user details
Out-of-band channel exchange	• Artifact Resolve request with **SAML Artifact** (received from IdP)	• IdP returns SAML Assertion containing o User **NRIC/FIN** (in SAML Subject tag in assertion) o **PasswordProtectedTransport/ MobileTwoFactorUnregistered / TimeSyncToken / SoftwarePKI**: These values represent the authentication mechanism used by the end user while logging in. This is contained in SAML AuthnContext tag in assertion. For more details please refer to Annexure D for the AuthnContext statements) o **Attributes:** Assertion returned after CorpPass authentication contains attributes that contain the authorization XMLs that represent the user roles. Every assertion returned after successful CorpPass authentication contains

Authentication Step	Parameters Sent (from SP to IdP)	Parameters Returned (from IdP to SP)
		▪ Attribute that contains User information in the <UserInfo> element; and ▪ Attribute that contains CorpPass Authorization XML in the <AuthAccess> element, that provides role(s) authorized for the user for that Digital Service along with any additional parameters for the Digital Service (if required). This is a mandatory attribute i.e. every assertion will contain one such attribute. ▪ If the user belongs to a third party entity, an additional attribute in the <TPAuthAccess> element is included in the assertion that provides details of the client entity that the user is authorized to provide third party services along with role(s) authorized for the user for that Digital Service and any additional parameters for the Digital Service (if required). The number of rows in the XML will vary depending on the number of clients that the user is authorized to perform third party services. This is not a mandatory attribute i.e. this attribute will be only present for users of a third party entity only. For more details please refer to Annexure B about CorpPass Authorization XMLs.

4.4.3 CorpPass XMLs

As described in the flow above, when a user uses the CorpPass authentication and authorization flow to login to a Digital Service, the identity provider should not only supply the user principal information (i.e. NRIC of the user) but also provide additional authorization information specific to the Digital Service

the user is logging into, the entity that the user is associated with and the role that the user has for that Digital Service.

User information, Authorization and Third-Party Authorisation information is always present in the <Attribute> statement with “urn:oasis:names:tc:SAML:2.0:assertion” as the Namespace in the assertion response that identity provider provides to the service provider. In the federated authentication flow:

1. Step 8 during Artifact Response: After the user completes the authentication process an artifact is sent over the browser to the service provider. SP returns the artifact using the back channel (out-of-band) to IdP to retrieve the assertion with user details. The assertion will contain the 'System defined ID of the user' in the <Subject> element (NameID) while the <AttributeStatement> element contains the user’s information, authorization information in XML format (which provides the details of the role information of that user for the Digital Service that the user is authenticating to) and details of any third party assignments that the user might have for that Digital Service.
2. The XML in the <AttributeStatement> tag in assertion includes:
    a. The NRIC/FIN or Foreign ID of the user within the <UserInfo> element as “CPUID” attribute.
    b. The entity (UEN/non-UEN ID) that the user belongs to within the <AuthAccess> element
    c. The third party relationship authorisation within the <TPAuthAccess> element
    d. Digital Service ID of the Digital Service that the user is accessing
    e. The role the user has for that Digital Service and entity combination
    f. Sub-UEN and other additional information as mandated by that Digital Service in CorpPass

Please note that SAML assertions can contain multiple <AttributeStatement> elements in the assertion XML. CorpPass assertion will always have one <AttributeStatement> element with <UserInfo> and <AuthAccess> XML in it with the details of the authorization for the user.

Specific to Third-Party Authorization, <TPAuthAccess> XML would contain additional details of the authorization for the third-party user. Please also note that elements in <AuthAccess> will “NULL” for a specific scenario (i.e, Scenario 3) where user is only assigned with Third-Party Authorization and do not have ‘Golden Profile’ and ‘Explicit Assignment’ (**Refer to Annexure E**).

4.4.3.1 CorpPass User Info XML

This section provides the format of the XML used for providing the user info details in the assertion. This XML is used in **Step 8** mentioned in the sequence in **Section 4.1.1**.

The table below provides the description of the tags used within the user XML, please note that the <UserInfo> element is mandatory in all CorpPass SAML assertions:

Please note that non-mandatory tag means that the XML tag will only be present in case it has data and is not mandatorily required in the XML. Mandatory tags in the XML will always contain values (including string NULL). For more details please refer to Annexure B for XSD and example CorpPass User Info XML.

Tag Name	Tag Description	Data Type	Field Length	Mandatory
UserInfo	This the starting tag of the User Info XML	Tag	-	Yes
CPAccType	CorpPass account type i.e. if the user is a CorpPass Administrator, CorpPass Sub-Administrator or a CorpPass User	String	30	Yes
CPUID	NRIC, FIN or Foreign ID number of the user.	String	20	Yes
CPUID_Country	Country where the Identity Card of the user that was used for verification was issued	String	2	Yes
CPUID_FullName	Full Name of User	String	100	Yes
CPSystemUID	System defined ID of the user.	String	20	Yes
ISSPHOLDER	Indicates if the user is a SingPass holder i.e. the user has activated their CorpPass ID using SingPass (YES or NO)	String	3	Yes
CPEntID	Entity ID (UEN or non-UEN ID) of the entity to which the user belongs in CorpPass	String	10	Yes
CPEnt_Status	Status of the entity in CorpPass as provided by issuance agencies. The possible values for entity status are: • Registered • De-Registered • Withdrawn • Null (Specific for Non-UEN scenario)	String	20	Yes
CPEnt_TYPE	Type of Entity that the user belongs to. E.g. UEN, Non-UEN	String	10	Yes
CPNonUEN_RegNo	Entity registration number of Non-UEN entity which is entered during CorpPass Admin registration. Value will be **"NULL"** if user belongs to UEN entity.	String	15	Yes
CPNonUEN_Country	Country of incorporation of Non-UEN entity which is provided during CorpPass Admin registration. Value will be **"NULL"** if user belongs to UEN entity.	String	2	Yes

Tag Name	Tag Description	Data Type	Field Length	Mandatory
CPNonUEN_Name	Name of Non-UEN entity which is entered during CorpPass Admin registration. Value will be **"NULL"** if user belongs to UEN entity.	String	100	Yes

4.4.3.2 CorpPass User Authorization XML

This section provides the format of the Authorization XML used for providing the user authorization details in the assertion. This XML is used in **Step 8** mentioned in the sequence in **Section 4.1.1**.

The table below provides the description of the tags used within the authorization XML, please note that the <AuthAccess> element is mandatory in all CorpPass SAML assertions:

Please note that non-mandatory tag means that the XML tag will only be present in case it has data and is not mandatorily required in the XML. Mandatory tags in the XML will always contain values (including string NULL). For more details please refer to Annexure B for XSD and example CorpPass User Authorization XML.

Tag Name	Tag Description	Data Type	Field Length	Mandatory
AuthAccess	This the starting tag of the authorization XML	Tag	-	Yes
Result_Set	This tag marks the beginning of the Digital Service authorization result set	Tag	-	Yes
ESrvc_Row_Count	This value indicates the number of Digital Services for which the authorizations are present in the XML.	Integer	10	Yes
ESrvc_Result	This tag signifies the beginning of the authorization details for a specific Digital Service	Tag	-	Yes
CPESrvcID	ID of the Digital Service that is requesting the authorization	String	25	Yes
Auth_Result_Set	This tag signifies the beginning of the authorization result for the user	Tag	-	Yes
Row_Count	This tag provides the count of the number of rows included in the result set. E.g. If the user access to two sub-UENs within the same entity, the result set will contain two rows with the role information for each sub-UEN in one individual row	Integer	10	Yes
Row	This tag signifies the starting of the actual authorization values for a given sub-UEN for	Tag	-	Yes

Tag Name	Tag Description	Data Type	Field Length	Mandatory
	the user. There could be multiple Row tags in an XML depending on the result set			
CPEntID_SUB	Sub-UEN value of that entity to which the user is assigned the authorization. Sub-UEN is an optional attribute for a Digital Service and therefore can be NULL. In case an Digital Service authorization does not contain sub-UEN then the result set will contain only one Row. If a sub-UEN is defined as mandatory by the Digital Service administrator but no value was supplied, **"ERROR_MISSING_VALUE"** will be returned for the field.	String	32	No
CPRole	The role assigned to the user for that particular Sub-UEN	String	20	Yes
StartDate	The start date for validity of the role i.e. the date from which this role is valid for the user for that Digital Service	Date	10	Yes
EndDate	The end date for validity of the role i.e. the date at which this role is no longer valid for the user for that Digital Service	Date	10	Yes
Additional Parameters as Name-Value pairs	These are optional parameters defined by Digital Service administrator. These parameters will be populated as required. These parameters use a name-value pair format and will contain the "Digital Service defined name" from CorpPass in the name field. If a parameter is defined as mandatory by the Digital Service administrator but no value was supplied, **"ERROR_MISSING_VALUE"** will be returned for the field.	String	66	No

4.4.3.3 CorpPass Third Party Authorization XML

This section provides the format of the Authorization XML used for providing the third party authorization details of the user in the assertion. This XML is used in **Step 8** mentioned in the sequence in **Section 4.1.1**.

The table below provides the description of the tags used within the third-party authorization XML, please note that the <TPAuthAccess> element is optional and is only added to existing <UserInfo> and <AuthAccess> elements for third-party scenario:

Please note that non-mandatory tag means that the XML tag will only be present in case it has data and is not mandatorily required in the XML. Mandatory tags in the XML will always contain values (including string NULL). For more details please refer to Annexure B for XSD and example CorpPass User Authorization XML.

Tag Name	Tag Description	Data Type	Field Length	Mandatory
TPAuthAccess	This the starting tag of the authorization XML	Tag	-	Yes
CP_TPEntID	Entity ID (UEN or non-UEN ID) of the third party entity to which the user has been assigned the third party authorization in CorpPass	String	10	Yes
CP_TPEnt_Status	Status of the entity in CorpPass as provided by issuance agencies. The possible values for entity status are: • Registered • De-Registered • Withdrawn	String	20	Yes
CP_TPEnt_TYPE	Type of Entity that the user belongs to. E.g. UEN, Non-UEN	String	10	Yes
Result_Set	This tag marks the beginning of the Digital Service authorization result set	Tag	-	Yes
ESrvc_Row_Count	This value indicates the number of Digital Services for which the authorizations are present in the XML. This value will be set to 1.	Integer	10	Yes
ESrvc_Result	This tag signifies the beginning of the authorization details for a specific Digital Service	Tag	-	Yes
CPESrvcID	ID of the Digital Service that is requesting the authorization	String	25	Yes

Auth_Set	This tag signifies the beginning of the third party authorization results for the user	Tag	-	Yes
ENT_ROW_COUNT	Indicates the number of rows in the third party assignment. This is equal to the number of clients that the user is authorized as third party for that Digital Service	Integer	10	Yes
TP_Auth	This tag represents the third party authorization of the user for one client entity	Tag	-	Yes
CP_Clnt_ID	Contains the client entity ID	String	10	Yes
CP_ClntEnt_TYPE	Contains the client entity type i.e. UEN or Non-UEN	String	10	Yes
Auth_Result_Set	This tag signifies the beginning of the authorization assigned for that client entity for the user	Tag	-	Yes
Row_Count	This tag provides the count of the number of rows included in the result set. E.g. If the user access to two sub-UENs within the same entity, the result set will contain two rows with the role information for each sub-UEN in one individual row	Integer	10	Yes
Row	This tag signifies the starting of the actual authorization values for a given sub-UEN for the user. There could be multiple Row tags in an XML depending on the result set	Tag	-	Yes
CP_ClntEnt_SUB	Sub-UEN value of that third party entity to which the user is assigned the authorization. Sub-UEN is an optional attribute for an Digital Service and therefore can be NULL. In case a Digital Service authorization does not contain sub-UEN then the result set will contain only one Row. If a sub-UEN is defined as mandatory by the Digital Service administrator but no value was supplied,	String	32	No

	"ERROR_MISSING_VALUE" will be returned for the field.			
CPRole	The role assigned to the user for that particular Sub-UEN	String	20	Yes
StartDate	The start date for validity of the role i.e. the date from which this role is valid for the user for that Digital Service	Date	10	Yes
EndDate	The end date for validity of the role i.e. the date at which this role is no longer valid for the user for that Digital Service	Date	10	Yes
Additional Parameters as Name-Value Pairs	These are optional parameters defined by Digital Service administrator. These parameters will be populated as required. These parameters use a name-value pair format and will contain the "Digital Service defined name" from CorpPass in the name field. If a parameter is defined as mandatory by the Digital Service administrator but no value was supplied, **"ERROR_MISSING_VALUE"** will be returned for the field.	String	66	No

5. WHAT DO AGENCIES DO TO INTEGRATE WITH FEDERATION?

CorpPass transition team will work with agency to take the respective party through the exact steps of the federation process. Roughly, the typical process has these steps:

1. Environment Setup: This includes installation and configuration of service provider module using commercial off-the-shelf, open source or custom developed software.
2. Configuration of service provider integration with Identity Provider which include exchange of metadata with Identity Provider which includes:
    a. Provider ID (or Realm, depending on the protocol you are using)
    b. Profiles within the protocol to be supported
    c. Endpoint URLs for each of the profiles to be supported
    d. Public certificates for validating your digital signatures
    e. CA certificate for the server certificate in your point of contact server
    f. Method for client authentication of the SOAP connections (none, X.509,certificate), plus the CA certificate and Distinguished Name (DN) of the client certificate if needed
    g. Type, value range and semantics of the Subject field in the assertion
    h. Name, type, value range and semantics of any attributes to be included in the assertion
    i. Session timeouts and request/assertion lifetimes.
3. Test the configured application in staging to assure that the trust is properly established and the necessary settings for application integration are being provided.
4. After completing the testing in staging, the configuration will be setup in production environment.

The sections below provide more details around the requirements for integration with Identity Provider and the metadata that is required to be exchanged.

5.1 ENVIRONMENT SETUP

Agencies need to evaluate their IT Landscape to identify the Service Provider solution that they need to implement to integrate with CorpPass. Regardless of the Service Provider software chosen, the steps involved in setting up service provider will typically include:

1. Installation of federated identity management software.
2. Configuration of federated identity management software as service provider.
3. Exchange metadata to establish trust connection with identity provider.

5.2 SERVICE PROVIDER CONFIGURATION AND INTEGRATION WITH IDP

This section provides the high-level overview of the details that are required to be configured in Service Provider module to enable integration with Identity Provider.

Please note that this information is provided to assist agencies in planning and setting up the SP environment. For the actual transition, a more detailed worksheet with detailed instructions will be provided to agencies using transition checklist process to enable the agencies to provide the actual information to SPCP team.

Parameter	Description	Value
Federation Name	This is the name of the federation that you are setting up in Service Provider. Please use the following naming format: "SPCP_<Agency ID>_<E-SRVC ID>_saml20fed".	
Provider ID	The URL of the Identity Provider. This will be provided by SPCP project to the agencies.	
Point of Contact Server	This is the same as above i.e. URL of the Identity Provider.	
Metadata File	Path the Metadata File that you have received from Identity Provider. This will be provided by SPCP project to the agencies.	
Signing Key	Select the key that you will be using to digitally sign the SAML messages that are exchanged with Identity Provider. Please refer to the next table for more details on certificates required for SAML.	
Encryption Key	Select the key that you will be using to decrypt the SAML messages received from Identity Provider. Please refer to the next table for more details on certificates required for SAML.	
SSL Server Authentication Certificate	This is the certificate that is received from Identity Provider for SSL mutual authentication. This certificate is used to authenticate the server during SAML exchange. This will be provided by SPCP project to the agencies.	SSL certificate used will be WAF certificate.
SSL Client Authentication Certificate	This is Service Provider's SSL certificate. This certificate (public key) needs to be shared with Identity Provider (CorpPass) so that IdP can authenticate the SP server during SAML exchange.	Not applicable to CorpPass system.
Signing Algorithm	This is the algorithm used for digital signatures. CorpPass will use RSA-SHA256 for digital signatures.	
Encryption Algorithm	This is the algorithm used for encryption. CorpPass will use AES-256-CBC for encryption. This is used in conjunction with RSA-1.5 which is used to encrypt the AES symmetric key. (For more details please refer to Annexure A – 7.3 Sample message flow.)	

Parameter	Description	Value
SAML Assertion Settings	This setting allows you to define how SAML assertions are processed by Service Provider. Please set the values to indicate that all assertion attributes are encrypted. Use the Identity Mapping file provided by SPCP to identify the attributes that are used in assertion for CorpPass	
Identity Mapping	Agencies will receive this information as part of the metadata from SPCP. Please import the identity mapping from SPCP in your service provider module to map the attributes in SAML assertion.	
Session Timeout (seconds)	Set the session timeout setting to the value provided by SPCP. The project will share this information as part of transition process.	Not applicable to CorpPass system. However, the artifact lifetime is configured as 600.
Logout Request Lifetime (seconds)	Set the logout request lifetime setting to the value provided by SPCP. The project will share this information as part of transition process.	Not applicable to CorpPass system.

5.3 CRYPTOGRAPHIC MATERIAL MANAGEMENT

This section outlines the certificates that Service Provider (agency) needs to obtain to setup federation with CorpPass. The table below lists the certificates required and the purpose for each certificate.

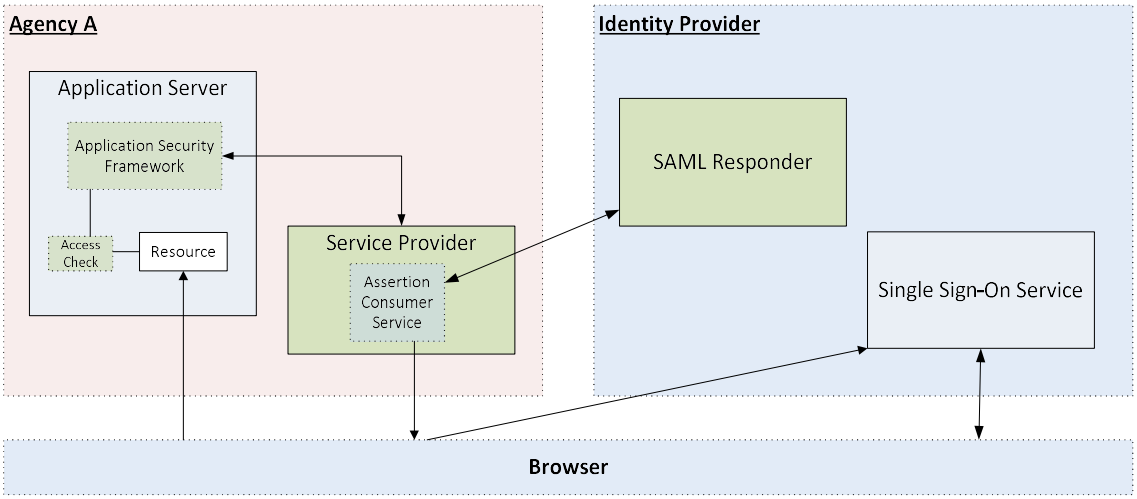
Certificate Type	Description
1 X.509 Certificate for digital signature of SAML Messages	This certificate is used for digital signatures of SAML messages exchanged with IdP
1 X.509 Certificate for encryption of SAML Messages	This certificate is used for encryption and decryption of SAML messages. Public Key of this certificate is shared with IdP to enable IdP to encrypt the messages. SP will decrypt the messages using the Private Key from this key pair

5.4 INTEGRATE APPLICATIONS WITH SERVICE PROVIDER

The steps of integrating applications with service provider is depend on the federated software that agency used. Generally, integrating applications with service provider involve the following steps:

1. Disable the existing login form.
2. Equip application with capability to receive user information from service provider.
3. Change the application logout call.
4. Modify on application idle timeout if necessary.

The diagram below shows a typical architecture of how applications are integrated with Service Provider and also shows Service Provider integration with Identity Provider



5.5 Out-of-band Channel Integration with CorpPass

CorpPass Identity Provider uses IdP initiated Artifact Resolution profile in SAML to authenticate CorpPass identities. This requires the use of out-of-band channel for exchanging the artifact for assertion containing the user's identity details.

CorpPass supports out-of-band connection using Internet only. Internet out-of-band channel uses one-way SSL i.e. identity of CorpPass IdP server is authenticated by agency server (using our CDN SSL certificate) and not vice-versa. Please note that over Internet out-of-band channel agencies are connecting to CorpPass through our WAF (Web Application Firewall) and the SSL certificate presented will be WAF certificate.

5.6 Establishing Federation with CorPass for Private Organizations

Private organizations that are integrating with CorpPass authentication using federation would follow the same arrangement as government agencies and use Internet out-of-band channel communication for fetching the assertion.

CorpPass Authentication interface specification requires the use of out-of-band back channel for artifact resolution service to ensure that user details are not sent over user's browser.

6. TECHNOLOGY LANDSCAPE

6.1 VENDOR LANDSCAPE

Please note that this section is provided for informational purposes only and the products, vendors and technologies mentioned in this section are neither endorsed nor recommended by SPCP for Service Provider Implementation. Agencies are required to evaluate the suitability of software based on their Digital Service specific requirements before identifying the solution for implementation.

On boarding agencies are required to perform evaluation and assessment based on agency's requirement and landscape to decide the software that fulfilled the needs.

Refer to the table below for capabilities required by the agency service provider module to support Federated Authentication using CorpPass.

Feature
Web SSO, <Response>, HTTP artifact
Artifact Resolution, SOAP
Name Identifier Management, HTTP redirect (IdP-initiated)
Name Identifier Management, SOAP (IdP-initiated)
Single Logout (IdP-initiated) – HTTP redirect
Single Logout (IdP-initiated) – SOAP
Single Logout (SP-initiated) – HTTP redirect
Single Logout (SP-initiated) – SOAP

Table below provides a quick reference of some of the popular vendors that provide software that can be used for setting up Service Provider Module.

Product Name	**Project/Vendor**
ADFS 3.0	Microsoft
CA Federation Manager	CA
DirX Access	Atos/Siemens
Entrust GetAccess	Entrust
Entrust IdentityGuard	Entrust
Horizon App Manager	VMware
NetIQ Access Manager	NetIQ (formerly Novell)

Product Name	Project/Vendor
Oracle Identity Federation 11g	Oracle
PingFederate	Ping Identity
RSA Federated Identity	RSA
Symplified	Symplified
Tivoli Federated Identity Manager	IBM

* Please note that some products features and abilities may have been updated. On boarding agency should check the website information of the originating product for the latest features and updates.

6.2 OPEN SOURCE

Please refer to the table below for reference of open source application that have the capability to configure as service provider or service provider lite:

Product Name	Project/Vendor
adAS	PRiSE
Larpe	Entrouvert
OpenAM	ForgeRock (ex. Sun)
SimpleSAMLphp	UNINETT AS

* Please note that some products features and abilities may have been updated. On boarding agency should check the website information of the originating product for the latest features and updates.

6.3 CUSTOM DEVELOPMENT

Agencies have the option to build the capability of service provider using custom development in order to integrate with CorpPass for Federated Authentication. The custom build service provider should follow the SAML2.0 specification stated in OASIS published standards, refer to https://www.oasis-open.org/standards for the complete SAML2.0 OASIS Standard Set.

7. ANNEXURE A

7.1 SAML 2.0 ARTIFACT SPECIFICATION

In general, a SAML 2.0 artifact is defined as follows:

```
SAML_artifact := B64 (TypeCode EndpointIndex RemainingArtifact)
TypeCode      := Byte1Byte2
EndpointIndex := Byte1Byte2
```

Thus a SAML 2.0 artifact consists of three components: a two-byte TypeCode, a two-byte EndpointIndex, and an arbitrary sequence of bytes called the RemainingArtifact. These three pieces of information are concatenated and base64-encoded to yield the complete artifact.

The TypeCode uniquely identifies the artifact format. SAML 2.0 predefines just one such artifact, of type 0x0004. The EndpointIndex is a reference to a particular artifact resolution endpoint managed by the artifact issuer (which may be either the IdP, as mentioned earlier). The RemainingArtifact, which is determined by the type definition, is the "meat" of the artifact.

The format of a type 0x0004 artifact is further defined as follows:

```
TypeCode          := 0x0004
RemainingArtifact := SourceId MessageHandle
SourceId          := 20-byte_sequence
MessageHandle     := 20-byte_sequence
```

Thus a type 0x0004 artifact is of size 44 bytes (unencoded). The SourceId is an arbitrary sequence of bytes, although in practice, the SourceId is the SHA-1 hash of the issuer's entityID. The MessageHandle is a random sequence of bytes that references a SAML message that the artifact issuer is willing to produce on-demand.

For example, consider this hex-encoded type 0x0004 artifact:

```
00040000064999557525854 75c37eee9f0ab6abae3f6422de436913660e3e917549a59709fd8c91f2
120222f
```

The TypeCode (0x0004) and the EndpointIndex (0x0000) are at the front of the artifact. The next 20 bytes are the SHA-1 hash of the issuer's entityID (https://saml.corppass.gov.sg/FIM/sps/CorpIDPFed/saml20) followed by 20 random bytes. The base64-encoding of these 44 bytes is in the ArtifactResolveRequest example above.

7.2 SAML 2.0 ARTIFACTRESOLVE EXAMPLE

The following example is taken from staging environment where SP would need to send to CorpPass via the Internet OOB channel as a SOAP message.


```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header/>
    <soapenv:Body>
        <samlp:ArtifactResolve xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="http://172.12.11.61:9080/sps/CorpIDPFed/saml20/soap" ID="FIMREQ_31438e67-0152-1a60-ba08-f97b302bc9d5" IssueInstant="2016-01-11T15:17:36Z" Version="2.0">
            <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://stg-home.authgateway.gov.sg/FIM/sps/EServiceSP/saml20</saml:Issuer>
            <ds:Signature Id="uuid31438e68-0152-1fbf-b678-f97b302bc9d5">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                    <ds:Reference URI="#FIMREQ_31438e67-0152-1a60-ba08-f97b302bc9d5">
                        <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#">
                                <xc14n:InclusiveNamespaces xmlns:xc14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="samlp saml ds"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>BiIj58mRQT/k3a+6xdTC29r/bAjOocMjTM1boFBl8g4=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
    <ds:SignatureValue>LbA2yppHQljjGO8kv3Pe8Zp1ew4Y/eIC7AXGHUK7F7JX+S6Rx6h93hn0FIDWDIuTr/Lj6hdMR6Db02dGrsr1RKwaSdi0rWYhUXnGQvFvxzhUjc2tBkw1975Pw5E02i19f7q1aJCNUJEpCo4HL5SIA2iW/1LPpfO4oAmvTgXJnIC3LZjl6InQlaLj6ACfGiq6X/7T1Dfy8bLsbV6h98Z5Ha3KPCxgIIAzJkGDRoovcxC2SrEl+JojA0whWrmWl41GpFY1bpKwPVbkSyryAY3ZGmwi+C3yQM5g3ZVhS1Kwa/MoJzKzufnPjQ0sTKQmBnp4eDwJHkBvBNd84wZf6h3LTg==</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:X509Data>
    <ds:X509Certificate>MIIFOTCCBCGgAwIBAgIMZ7x3mwAAAABJ0bdnMA0GCSqGSIb3DQEBBQUAME0xCzAJBgNVBAYTAlNHMSgwJgYDVQQKEx9OZXRydXN0IENlcnRpZmljYXRlIEF1dGhvcml0eSAxMRQwEgYDVQQLEwtOZXRydXN0IENBMTAeFw0xNTAyMTMwNDQ5NTBaFw0xODAyMTMwNTE5NTBaMIGiMQswCQYDVQQGEwJTRzEoMCYGA1UEC
```

```
hMfTmV0cnVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgMTEdMBsGA1UECxMUTmV0cnVzdCBDQTEgKFNlcnZlcikxHD
AaBgNVBAsTE01pbmlzdHJ5IG9mIEZpbmFuY2UxGTAXBgNVBAsTEFNpbmdQYXNzIEdhdGV3YXkxETAPBgNVBAMTCH
N0Zy1zYW1sMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvYfGDb+4eiaTsl93FqwTzixulQhVm6n2Zc3ccjnYK
LrySGWXgsQw1NwjkCm5KQyew0kEH7zbmum7POlUpB9rPqrsLiOVEsPwSXnlDumhRs3s+q5iBu5BpsXwiB25d06yuuaaZ4
a5jnCW/KkAAKkfdPj1W7TYmwtNR5Zrg/AhFCSSvENJ4KB/CETbvM7gKX+csDxtt10MV1nnMJZwNFuiVWcEQco5yRKTn/O
+TNt2bNQYyp+Oyw0LndzjgUSnVMeInqTaAiQEJ4GC5+Bjl8dKnIg/As+J6DjJmU/kaDXpr/VumQfPfnLF1+b/CE2NMmUqdhH
a2XnFuPT0ztaHVOf0xQIDAQABo4IBwTCCAb0wCwYDVR0PBAQDAgeAMBUGA1UdIAQOMAwwCgYIKoU+AIdqBgEwWA
YJYIZIAYb6ax4BBEsMSVRoZSBwcml2YXRlIGtleSBjb3JyZXNwb25kaW5nIHRvIHRoaXMgY2VydGlmaWNhdGUgbWF5IGh
hdmUgYmVlbiBleHBvcnRlZC4wgakGA1UdHwSBoTCBnjBloGOgYaRfMF0xCzAJBgNVBAYTAlNHMSgwJgYDVQQKEx9OZ
XRydXN0IENlcnRpZmljYXRlIEF1dGhvcml0eSAxMRQwEgYDVQQLEwtOZXRydXN0IENBMTEOMAwGA1UEAxMFQ1JMO
TcwNaAzoDGGL2h0dHA6Ly9uZXRydXN0Y29ubmVjdG9yLm5ldHJ1c3QubmV0L25ldHJ1c3QuY3JsMCsGA1UdEAQkMCK
ADzIwMTUwMjEzMDQ0OTUwWoEPMjAxODAyMTMwNTE5NTBaMB8GA1UdIwQYMBaAFB1EibJFJn9va5LFOntyY8rScCr
dMB0GA1UdDgQWBBS26O+ONM6S0dzh7zsg55rrxg3i2DAJBgNVHRMEAjAAMBkGCSqGSIb2fQdBAAQMMAobBFY4LjE
DAgSwMA0GCSqGSIb3DQEBBQUAA4IBAQBRVVDtvyYU93aJ5cQ59pmupTD2t1DhzxFuQid+OUCP95OFx5fTTX2/Od5fks
phI4/l3bMeheNICRsNvCBjFke0CqttFPhWVEAUzm7DhZEIIyn3mhEuYsTT9+uL3b5p2dnZZJMqcW9e2V9kFodlsMRcLH3UT
W+kxoYm1G9evwlVCUXIsV++BL9FRe6jFv8QuDXYztmcEhp6jHAcbDPN3K9ISzG9hD4N2u6jGwWpWw9AZcRWsnKzUguJ
8d5acbfPnl89anb7hG2uq0teh9JSKNkYXmhyau44NWBwU88cLkRJSZUYxtzaGUztTgtLFLnaDx2+4Fwa2uuPdZKYngjPh8N/
</ds:X509Certificate>
                                        </ds:X509Data>
                                    </ds:KeyInfo>
                                </ds:Signature>

        <samlp:Artifact>AAQAAFDAXYQm+WRGiqG7dPVRA3qTT3OZhyNDw0UPl0Z6j8leYsBbyup6iNs=</samlp:Artifact
>
                    </samlp:ArtifactResolve>
        </soapenv:Body>
</soapenv:Envelope>
```

7.3 SAML 2.0 ARTIFACTRESPONSE ENCRYPTED EXAMPLE

The sample assertion shown in below depicts the encrypted SAML assertion message. To decrypt the encrypted SAML assertion message, SP would need to perform 2 levels of decryptions.

1. **RSA Encrypted Cipher Text**
   a. Perform RSA decryption to obtain the AES symmetric key
2. **AES Encrypted Cipher Text**
   a. Perform AES decryption to obtain the plain text which contains the NAMEID parameter (i.e. 'System defined ID of the user'), <UserInfo> contains NRIC/FIN or Foreign ID as “CPUID” attribute and <AuthAccess>
   b. Specific to Third-Party Authorisation, the decrypted text would contain <TPAuthAccess> element.

```
<samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Destination="https://stg-
home.eservice.gov.sg/FIM/sps/EServiceSP/saml20/login" ID="FIMRSP_b65b309-0155-1e61-8813-adf581bcef2e"
IssueInstant="2016-06-01T09:57:42Z" Version="2.0">
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://stg-
saml.corppass.gov.sg/FIM/sps/CorpIDPFed/saml20</saml:Issuer>
        <ds:Signature Id="uuidb65b30a-0155-1b27-a7a5-adf581bcef2e">
```

```
                <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                        <ds:Reference URI="#FIMRSP_b65b309-0155-1e61-8813-adf581bcef2e">
                                <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#">
                                                <xc14n:InclusiveNamespaces
xmlns:xc14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="samlp xs saml xsi ds"/>
                                        </ds:Transform>
                                </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

        <ds:DigestValue>0xh3m9nEP/K1Z7iyMaH3uZpGB+ngejgtqhMHnswo3kI=</ds:DigestValue>
                        </ds:Reference>
                </ds:SignedInfo>

        <ds:SignatureValue>C1DYfRCEkyoQ/EbgvbOCtckUJrCSiBYp/zQcoNsc9t4wCyS7c2HwcNgBxJlYwenvtkBzAp8B
kS8WMsnJFsDuMyNsvaAbNdLLYucsKYGPK5WpoW1S57PQqof7KVU9uyeIRhhqPgz1TuNsKisM5di4vTeEYdzRI5l+ptLpZ/
cdR4H62qcZugCtLpadRG+eN5earfb4nn2bDhiQKa+xQY+jlBJE4MCEWf91jl7eFTY/Cux1oeL5+IG+rXneXh4VdpLaOpIk1O4
VIQU8WTrMTvMT0K0MhtycpM33Mjlns9JpL82TBSw1qK/jidkOGCJacSyVI0sFWndZnoViUasNHU1Qtw==</ds:SignatureVal
ue>
                <ds:KeyInfo>
                        <ds:X509Data>

        <ds:X509Certificate>MIIFOzCCBCOgAwIBAgIMTYaR2AAAAABJ0kTtMA0GCSqGSIb3DQEBCwUAME0xCzAJBg
NVBAYTAlNHMSgwJgYDVQQKEx9OZXRydXN0IENlcnRpZmljYXRlIEF1dGhvcml0eSAxMRQwEgYDVQQLEwtOZXRydXN
0IENBMTAeFw0xNjAxMjIwNDEyNTJaFw0xOTAxMjIwNDQyNTJaMIGjMQswCQYDVQQGEwJTRzEoMCYGA1UEChMfTm
V0cnVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgMTEdMBsGA1UECxMUTmV0cnVzdCBDQTEgKFNlcnZlcikxHDAaBgN
VBAsTE01pbmlzdHJ5IG9mIEZpbmFuY2UxETAPBgNVBAsTCENvcnBQYXNzMRowGAYDVQQDExFzdGctc2FtbC1jb3Jwc
GFzczCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL8ocP1T0kRyTYYJ297BY4vEfURaj2RR/wnwVUAGKh
PC7h+iZ+9uT3V3JqS15Yg2XVH5d+wx2SlvRP9iZtRKec005oFor4cpYdyfGPp6go2j9yzbaz7hE9uljf09G1zdb/f00takohUrHW
4iOTQT01shthA6IPi97dd0i8G6knElMgCxXsj1e4qQoBqd8JXZ1bUvSV49GpuWFuSRN4VVC+Lhy5qhiJLvAoPM2YdZR7M1
U3tr7P1i//Wzu2/QhSvLc5oo134YP0m3rfNaUsCo0jXapm/VBS9WL+kHkbtH5Ogg6tm1m0tnTlsgRifbmD8Hs2S5bJ7a8TAaZe
CKnLm5kNkCAwEAAaOCAclwggG+MAsGA1UdDwQEAwIHgDAVBgNVHSAEDjAMMAoGCCqFPgCHagYBMFgGCWCGS
AGG+mseAQRLDElUaGUgcHJpdmF0ZSBrZXkgY29ycmVzcG9uZGluZyB0byB0aGlzIGNlcnRpZmljYXRlIG1heSBoYXZlIGJl
ZW4gZXhwb3J0ZWQuMIGqBgNVHR8EgaIwgZ8wZqBkoGKkYDBeMQswCQYDVQQGEwJTRzEoMCYGA1UEChMfTmV0c
nVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgMTEUMBIGA1UECxMLTmV0cnVzdCBDQTExDzANBgNVBAMTBkNSTDE
xNzA1oDOgMYYvaHR0cDovL25ldHJ1c3Rjb25uZWN0b3IubmV0cnVzdC5uZXQvbmV0cnVzdC5jcmwwKwYDVR0QBCQwIo
APMjAxNjAxMjIwNDEyNTJagQ8yMDE5MDEyMjA0NDI1MlowHwYDVR0jBBgwFoAUHUSJskUmf29rksU6e3JjytJwKt0wHQ
YDVR0OBBYEFKwDusz8JUFsQdABpkiZwLYn5nJ2MAkGA1UdEwQCMAAwGQYJKoZIhvZ9B0EABAwwChsEVjguMQMCB
LAwDQYJKoZIhvcNAQELBQADggEBABx+rXkisYGMEVNZD5Ms68nCSJZhkgta9e7PFf4nVQWe1sBAMPqUGd5zZseMpzX
Li48lO3x1qUDWQX7/MFO1Wbq1U/JFzI4Ld7E2+7PjH4H4ucwDS/XcXKjp8Sk+pj5qn7klVYG+4zX4SNV/IZ9Qh7II3DXoRnQ
7/8LNGGn4zodyYsYfJKfnnK7sJXpvcIuvVbbBSP1h749/5pe99njaZ6n/4DJ5DeKWheApPwVKtTzi7BtGRnmUMiY1ITrTj5jHhA
2i3vqK5P/SCpiBa+iJp5zMyco0VeBwUeTwhPZdMya50P8MuLkJjmXaG0Bw+FdmXa0HP+ksXSFS62cqEvdID+A=</ds:X509
Certificate>
                        </ds:X509Data>
                </ds:KeyInfo>
        </ds:Signature>
```

```
<samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<saml:EncryptedAssertion>
        <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#" Id="uuidb65b2ea-0155-1bde-8993-adf581bcef2e" Type="http://www.w3.org/2001/04/xmlenc#Element">
                <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                <ds:KeyInfo>
                        <EncryptedKey Id="uuidb65b2eb-0155-1cf1-9c9a-adf581bcef2e">
                                <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                                <ds:KeyInfo>
                                        <ds:KeyName>CN=stg-saml, OU=eService Gateway, OU=Ministry of Finance, OU=Netrust CA1 (Server), O=Netrust Certificate Authority 1, C=SG</ds:KeyName>
                                </ds:KeyInfo>
                                <CipherData>
                                        <CipherValue> xxxRSA Encrypted Cipher Textxxx </CipherValue>
                                </CipherData>
                        </EncryptedKey>
                </ds:KeyInfo>
                <CipherData>
                        <CipherValue> xxxAES Encrypted Cipher Textxxx </CipherValue>
                </CipherData>
        </EncryptedData>
</saml:EncryptedAssertion>
</samlp:Response>
```

7.4 SAML 2.0 ARTIFACTRESPONSE DECRYPTED EXAMPLE

The sample assertion shown below depicts the plain-text SAML assertion message. The User Information and authorisation XML found in the <saml:AttributeStatement> element is Base64 encoded. To obtain the required XML, SP would need to perform Base64 decode.


```
<samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Destination="https://stg-home.eservice.gov.sg/FIM/sps/EServiceSP/saml20/login" ID="FIMRSP_9e01e03-0155-1120-8d57-ff2e432a7581" IssueInstant="2016-06-01T02:52:10Z" Version="2.0">
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://stg-saml.corppass.gov.sg/FIM/sps/CorpIDPFed/saml20</saml:Issuer>
    <ds:Signature Id="uuid9e01e04-0155-1680-9c06-ff2e432a7581">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#FIMRSP_9e01e03-0155-1120-8d57-ff2e432a7581">
                <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#">
                        <xc14n:InclusiveNamespaces xmlns:xc14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="samlp xs saml xsi ds"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

    <ds:DigestValue>N/Mt7vU2kkc97twmFsyrCE3GYNi2PJpqu07Sh557ny0=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>

    <ds:SignatureValue>pW8iwgYHseoN+xuKBtygTemud1CMrefn0L6t+HNC1RALndt7I3z46WNB/C03y+4pT4aznR7CiZNDwJjEh081KIvj3+LNW9y93CF8NjQXkLmg+A0XCxKRKL1N7h8eiGIST/MFOzvAFXavLPvQtcbXYUbo9GA0JHuwoFA+s+4VrpR1bbMqhxFKrCQGkGmnOhm9SPxVP3BZ59B5nozfzWenjWUA8fnD3/PuvOboEt+bFD//Av50qibghneN9x+GV/iCaZVB7BcY6LMyOt6jfSG5HuCdaS+dzvByRFYgpzAnkkOsvpSC4Z7U0mqrdLeXTH6Bmlf4lafPEna2sWDgY05aOQ==</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>

    <ds:X509Certificate>MIIFOzCCBCOgAwIBAgIMTYaR2AAAAABJ0kTtMA0GCSqGSIb3DQEBCwUAME0xCzAJBgNVBAYTAlNHMSgwJgYDVQQKEx9OZXRydXN0IENlcnRpZmljYXRlIEF1dGhvcml0eSAxMRQwEgYDVQQLEwtOZXRydXN0IENBMTAeFw0xNjAxMjIwNDEyNTJaFw0xOTAxMjIwNDQyNTJaMIGjMQswCQYDVQQGEwJTRzEoMCYGA1UEChMfTmV0cnVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgMTEdMBsGA1UECxMUTmV0cnVzdCBDQTEgKFNlcnZlcikxHDAaBgNVBAsTE01pbmlzdHJ5IG9mIEZpbmFuY2UxETAPBgNVBAsTCENvcnBQYXNzMRowGAYDVQQDExFzdGctc2FtbC1jb3JwcGFzczCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL8ocP1T0kRyTYYJ297BY4vEfURaj2RR/wnwVUAGKhPC7h+iZ+9uT3V3JqS15Yg2XVH5d+wx2SlvRP9iZtRKec005oFor4cpYdyfGPp6go2j9yzbaz7hE9uljf09G1zdb/f00takohUrHW4iOTQT01shthA6IPi97dd0i8G6knElMgCxXsj1e4qQoBqd8JXZ1bUvSV49GpuWFuSRN4VVC+Lhy5qhiJLvAoPM2YdZR7M1U3tr7P1i//Wzu2/QhSvLc5oo134YP0m3rfNaUsCo0jXapm/VBS9WL+kHkbtH5Ogg6tm1m0tnTlsgRifbmD8Hs2S5bJ7a8TAaZe
```

CKnLm5kNkCAwEAAaOCAclwggG+MAsGA1UdDwQEAwIHgDAVBgNVHSAEDjAMMAoGCCqFPgCHagYBMFgGCWCGS
AGG+mseAQRLDElUaGUgcHJpdmF0ZSBrZXkgY29ycmVzcG9uZGluZyB0byB0aGlzIGNlcnRpZmljYXRlIG1heSBoYXZlIGJl
ZW4gZXhwb3J0ZWQuMIGqBgNVHR8EgaIwgZ8wZqBkoGKkYDBeMQswCQYDVQQGEwJTRzEoMCYGA1UEChMfTmV0c
nVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgMTEUMBIGA1UECxMLTmV0cnVzdCBDQTExDzANBgNVBAMTBkNSTDE
xNzA1oDOgMYYvaHR0cDovL25ldHJ1c3Rjb25uZWN0b3IubmV0cnVzdC5uZXQvbmV0cnVzdC5jcmwwKwYDVR0QBCQwIo
APMjAxNjAxMjIwNDEyNTJagQ8yMDE5MDEyMjA0NDI1MlowHwYDVR0jBBgwFoAUHUSJskUmf29rksU6e3JjytJwKt0wHQ
YDVR0OBBYEFKwDusz8JUFsQdABpkiZwLYn5nJ2MAkGA1UdEwQCMAAwGQYJKoZIhvZ9B0EABAwwChsEVjguMQMCB
LAwDQYJKoZIhvcNAQELBQADggEBABx+rXkisYGMEVNZD5Ms68nCSJZhkgta9e7PFf4nVQWe1sBAMPqUGd5zZseMpzX
Li48lO3x1qUDWQX7/MFO1Wbq1U/JFzl4Ld7E2+7PjH4H4ucwDS/XcXKjp8Sk+pj5qn7klVYG+4zX4SNV/lZ9Qh7II3DXoRnQ
7/8LNGGn4zodyYsYfJKfnnK7sJXpvcluvVbbBSP1h749/5pe99njaZ6n/4DJ5DeKWheApPwVKtTzi7BtGRnmUMiY1ITrTj5jHhA
2i3vqK5P/SCpiBa+iJp5zMyco0VeBwUeTwhPZdMya50P8MuLkJjmXaG0Bw+FdmXa0HP+ksXSFS62cqEvdID+A=</ds:X509
Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<saml:Assertion ID="Assertion-uuid9e01dd4-0155-173b-918f-ff2e432a7581" IssueInstant="2016-06-
01T02:52:10Z" Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://stg-
saml.corppass.gov.sg/FIM/sps/CorpIDPFed/saml20</saml:Issuer>
<ds:Signature Id="uuid9e01dd5-0155-184e-bed8-ff2e432a7581">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
<ds:Reference URI="#Assertion-uuid9e01dd4-0155-173b-918f-ff2e432a7581">
<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#">
<xc14n:InclusiveNamespaces
xmlns:xc14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs saml xsi"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>5eiFjcVKQTgvjpF/P6rlUmdH6QyK1ODilQNC1wu3tiw=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>HVnjbonSPau5Rz0n/o6WPkz003EYdVqQpAD3BZ+LQKtu+YuydpO+IYNw+xBNP972Y0xhX
1gI90m1Du7sC6ytkOLgJlXdcerXU2FR1BlDtg5MLxpNh06jjZpHASYxuq3WaCHyTw2fF/20lp4QhfGsjgGhSzomWX5zzw1teA
94G3BEqP/34+A+Ex0Z9HFNnbUO8Iu+F1X2WG4YTnLZ7UMIA8xEFXZP0gu0rI1J7WYE3pGSZ5qxa/ywitCmKWrIlZCAsjZd

5S1kdsznH/Wgy0k/rR2mKGDcfZe++5aV6VM9xwWaylHRPS/1et/Ha5sh7svkNKhWNdSvcrymJv7LADzXZA==</ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>MIIFOzCCBCOgAwIBAgIMTYaR2AAAAABJ0kTtMA0GCSqGSIb3DQEBCwUAME0xCzAJBgNVBAYTAlNHMSgwJgYDVQQKEx9OZXRydXN0IENlcnRpZmljYXRlIEF1dGhvcml0eSAxMRQwEgYDVQQLEwtOZXRydXN0IENBMTAeFw0xNjAxMjIwNDEyNTJaFw0xOTAxMjIwNDQyNTJaMIGjMQswCQYDVQQGEwJTRzEoMCYGA1UEChMfTmV0cnVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgMTEdMBsGA1UECxMUTmV0cnVzdCBDQTEgKFNlcnZlcikxHDAaBgNVBAsTE01pbmlzdHJ5IG9mIEZpbmFuY2UxETAPBgNVBAsTCENvcnBQYXNzMRowGAYDVQQDExFzdGctc2FtbC1jb3JwcGFzczCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL8ocP1T0kRyTYYJ297BY4vEfURaj2RR/wnwVUAGKhPC7h+iZ+9uT3V3JqS15Yg2XVH5d+wx2SIvRP9iZtRKec005oFor4cpYdyfGPp6go2j9yzbaz7hE9uljf09G1zdb/f00takohUrHW4iOTQT01shthA6IPi97dd0i8G6knElMgCxXsj1e4qQoBqd8JXZ1bUvSV49GpuWFuSRN4VVC+Lhy5qhiJLvAoPM2YdZR7M1U3tr7P1i//Wzu2/QhSvLc5oo134YP0m3rfNaUsCo0jXapm/VBS9WL+kHkbtH5Ogg6tm1m0tnTlsgRifbmD8Hs2S5bJ7a8TAaZeCKnLm5kNkCAwEAAaOCAclwggG+MAsGA1UdDwQEAwIHgDAVBgNVHSAEDjAMMAoGCCqFPgCHagYBMFgGCWCGSAGG+mseAQRLDElUaGUgcHJpdmF0ZSBrZXkgY29ycmVzcG9uZGluZyB0byB0aGlzIGNlcnRpZmljYXRlIG1heSBoYXZlIGJlZW4gZXhwb3J0ZWQuMIGqBgNVHR8EgaIwgZ8wZqBkoGKkYDBeMQswCQYDVQQGEwJTRzEoMCYGA1UEChMfTmV0cnVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgMTEUMBIGA1UECxMLTmV0cnVzdCBDQTExDzANBgNVBAMTBkNSTDExNzA1oDOgMYYvaHR0cDovL25ldHJ1c3Rjb25uZWN0b3IubmV0cnVzdC5uZXQvbmV0cnVzdC5jcmwwKwYDVR0QBCQwIoAPMjAxNjAxMjIwNDEyNTJagQ8yMDE5MDEyMjA0NDI1MlowHwYDVR0jBBgwFoAUHUSJskUmf29rksU6e3JjytJwKt0wHQYDVR0OBBYEFKwDusz8JUFsQdABpkiZwLYn5nJ2MAkGA1UdEwQCMAAwGQYJKoZIhvZ9B0EABAwwChsEVjguMQMCBLAwDQYJKoZIhvcNAQELBQADggEBABx+rXkisYGMEVNZD5Ms68nCSJZhkgta9e7PFf4nVQWe1sBAMPqUGd5zZseMpzXLi48lO3x1qUDWQX7/MFO1Wbq1U/JFzl4Ld7E2+7PjH4H4ucwDS/XcXKjp8Sk+pj5qn7klVYG+4zX4SNV/IZ9Qh7Il3DXoRnQ7/8LNGGn4zodyYsYfJKfnnK7sJXpvcIuvVbbBSP1h749/5pe99njaZ6n/4DJ5DeKWheApPwVKtTzi7BtGRnmUMiY1ITrTj5jHhA2i3vqK5P/SCpiBa+iJp5zMyco0VeBwUeTwhPZdMya50P8MuLkJjmXaG0Bw+FdmXa0HP+ksXSFS62cqEvdID+A=</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</ds:Signature>

<saml:Subject>

<saml:NameID Format="urn:ibm:names:ITFIM:5.1:accessmanager">***'System defined ID of the user' (i.e. CP1234)***</saml:NameID>

<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">

<saml:SubjectConfirmationData NotOnOrAfter="2016-06-01T03:02:10Z" Recipient="https://stg-home.eservice.gov.sg/FIM/sps/EServiceSP/saml20/login"/>

</saml:SubjectConfirmation>

</saml:Subject>

<saml:Conditions NotBefore="2016-06-01T02:42:10Z" NotOnOrAfter="2016-06-01T03:02:10Z">

<saml:AudienceRestriction>

<saml:Audience>https://stg-home.eservice.gov.sg/FIM/sps/EServiceSP/saml20</saml:Audience>

</saml:AudienceRestriction>

</saml:Conditions>

<saml:AuthnStatement AuthnInstant="2016-06-01T02:52:10Z" SessionIndex="uuid9dea368-0155-1105-8947-ff2e432a7581" SessionNotOnOrAfter="2016-06-01T03:52:10Z">

<saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>

</saml:AuthnContext>

```
                    </saml:AuthnStatement>
                    <saml:AttributeStatement>
                        <saml:Attribute                                    Name="22469300W"
NameFormat="urn:oasis:names:tc:SAML:2.0:assertion">
                            <saml:AttributeValue
xsi:type="xs:string">PFVzZXJJbmZvPg0KCTxDUEFjY1R5cGU+VXNlcjwvQ1BBY2NUeXBlPg0KCTxDUFVJRD5GMTlzNDU
2N1A8L0NQVUlEPg0KCTxDUFVJRF9Db3VudHJ5PlNHPC9DUFVJRF9Db3VudHJ5Pg0KCTxDUFVJRF9GdWxsTmFtZT5K
b2huIEdyaXNoYW08L0NQVUlEX0Z1bGxOYW1lPg0KCTxDUFN5c3RlbVVJRD5DUDE5MjwvQ1BTeXN0ZW1VSUQ+DQoJ
PEITU1BIT0xERVI+WUVTPC9JU1NQSE9MREVSPg0KCTxDUEVudEIEPII5MFNTMDAwMUE8L0NQRW50SUQ+DQoJPE
NQRW50X1N0YXR1cz5SZWdpc3RlcmVkPC9DUEVudF9TdGF0dXM+DQoJPENQRW50X1RZUEU+VUVOPC9DUEVudF9
UWVBFPg0KCTxDUE5vblVFTl9SZWdObz5OVUxMPC9DUE5vblVFTl9SZWdObz4NCgk8Q1BOb25VRU5fQ291bnRyeT5O
VUxMPC9DUE5vblVFTl9Db3VudHJ5Pg0KCTxDUE5vblVFTl9OYW1IPk5VTEw8L0NQTm9uVUVOX05hbWU+DQo8L1VzZX
JJbmZvPg0KPEF1dGhBY2Nlc3M+DQoJPFJlc3VsdF9TZXQ+DQoJCTxSb3dfQ291bnQ+MTwvRVNydmNfUm93
X0NvdW50Pg0KCQk8RVNydmNfUmVzdWx0Pg0KCQkJPENQRVNydmNJRD5CR0VTUlYxPC9DUEVTcnZjSUQ+DQoJCQ
k8QXV0aF9SZXN1bHRfU2V0Pg0KCQkJCTxSb3dfQ291bnQ+MjwvUm93X0NvdW50Pg0KCQkJCTxSb3c+DQoJCQkJCTx
DUEVudElEX1NVQj5OVUxMPC9DUEVudElEX1NVQj4NCgkJCQkJPENQUm9sZT5OVUxMPC9DUFJvbGU+DQoJCQkJCT
xTdGFydERhdGU+MjAxNi0wMS0xNTwvU3RhcnREYXRlPg0KCQkJCQk8RW5kRGF0ZT4yMDE2LTAyLTE1PC9FbmREYX
RlPg0KCQkJCQk8RVNydmNfUm93Pg0KCQkJCQk8Row8vU3RhcnREYXRlPg0KCQkJCQk8RW5kRGF0ZT4yMDE3LTA0LTE1PC9FbmREYX
RlPg0KCQkJCQk8RVNydmNfUm93Pg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9IlllYXIgb2YgY
XNzZXNzbWVudCI+MjAxNDwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDIiPnZhbHVlIDA
yPC9QYXJhbWV0ZXI+DQoJCQkJCTxQYXJhbWV0ZXIgbmFtZT0ib3RoZXIwMyI+dmFsdWUgMDM8L1BhcmFtZXRlcj4NCg
kJCQkJPFBhcmFtZXRlciBuYW1lPSJvdGhlcjA0Ij52YWx1ZSAwNDwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5
hbWU9Im90aGVyMDUiPnZhbHVlIDA1PC9QYXJhbWV0ZXI+DQoJCQkJCTxQYXJhbWV0ZXIgbmFtZT0ib3RoZXIwNiI+dmF
sdWUgMDY8L1BhcmFtZXRlcj4NCgkJCQkJPFBhcmFtZXRlciBuYW1lPSJvdGhlcjA3Ij52YWx1ZSAwNzwvUGFyYW1ldGVyP
g0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDgiPnZhbHVlIDA4PC9QYXJhbWV0ZXI+DQoJCQkJPC9Sb3c+CQo
JCQk8L0NlbnRfUmVzdWx0PgkJCTwvRVNydmNfUm93X0NvdW50PgkJPC9SZXN1bHRfU2V0Pg0KPC9RdXRoQWN
jZXNzPg==</saml:AttributeValue>
                            </saml:Attribute>
                    </saml:AttributeStatement>
                </saml:Assertion>
</samlp:Response>
```

8. ANNEXURE B

8.1 CORPPASS AUTHORIZATION XML FORMATS

This section provides the XSD and example XMLs for the CorpPass User Information, CorpPass User Authorization and CorpPass Third Party Authorization XMLs which will form the SAML payload.

8.1.1 CorpPass User Information XML

This section provides the XML Schema (XSD) and example XML for CorpPass User Info that will be shared from CorpPass IdP to the Digital Service as an attribute in SAML Assertion that is returned to Digital Service as part of CorpPass Authentication and Authorization.

Please note that this attribute will be mandatorily present in the assertion for all Digital Services using CorpPass, even if the Digital Service is using CorpPass for authentication only.

CorpPass User Info XSD:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
	<xs:element name="UserInfo">
		<xs:complexType>
			<xs:sequence>
				<xs:element type="xs:string" name="CPAccType" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPUID" maxOccurs="1" minOccurs="1"/> <!--CPv2.0: Attribute will have NRIC / FIN / Foreign ID number -->
				<xs:element type="xs:string" name="CPUID_Country" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPUID_FullName" minOccurs="1" maxOccurs="1"/> <!--CPv2.0: New attribute for user fullname-->
				<xs:element type="xs:string" name="CPSystemUID" minOccurs="1" maxOccurs="1"/> <!--CPv2.0: New attribute for Gemalto account running number-->
				<xs:element type="xs:string" name="ISSPHOLDER" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPEntID" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPEnt_Status" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPEnt_TYPE" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPNonUEN_RegNo" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPNonUEN_Country" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPNonUEN_Name" maxOccurs="1" minOccurs="1"/>
			</xs:sequence>
		</xs:complexType>
```

```
        </xs:element>
</xs:schema>
```

Example CorpPass User Info XML – Base64 Encoded:

```
PFVzZXJJbmZvPg0KCTxDUEFjY1R5cGU+VXNlcjwvQ1BBY2NUeXBlPg0KCTxDUFVJRD5GMTlzNDU2N1A8L0NQVUlEPg0KCTxDUFVJRF9Db3VudHJ5PlNHPC9DUFVJRF9Db3VudHJ5Pg0KCTxDUFVJRF9GdWxsTmFtZT5Kb2huIEdyaXNoYW08L0NQVUlEX0Z1bGxOYW1lPg0KCTxDUFN5c3RlbVVJRD5DUDE5MjwvQ1BTeXN0ZW1VSUQ+DQoJPEITU1BIT0xERVI+WUVTPC9JU1NQSE9MREVSPg0KCTxDUEVudEIEPII5MFNTMDAwMUE8L0NQRW50SUQ+DQoJPENQRW50X1N0YXR1cz5SZWdpc3RlcmVkPC9DUEVudF9TdGF0dXM+DQoJPENQRW50X1RZUEU+VUVOPC9DUEVudF9UWVBFPg0KCTxDUEVudF9UWVBFPg0KCTxDUE5vbVVFTl9SZWdObz5OVUxMPC9DUE5vbVVFTl9SZWdObz4NCgk8Q1BOb25VRU5fQ291bnRyeT5OVUxMPC9DUE5vbVVFTl9Db3VudHJ5Pg0KCTxDUE5vbVVFTl9OYW1lPk5VTEw8L0NQTm9uVUVOX05hbWU+DQo8L1VzZXJJbmZvPg==
```

Example UEN CorpPass User Info XML – Decoded:

```
<UserInfo>
        <CPAccType>User</CPAccType>
        <CPUID>F1234567P</CPUID>
        <CPUID_Country>SG</CPUID_Country>
        <CPUID_FullName>John Grisham</CPUID_FullName>
        <CPSystemUID>CP192</CPSystemUID>
        <ISSPHOLDER>YES</ISSPHOLDER>
        <CPEntID>R90SS0001A</CPEntID>
        <CPEnt_Status>Registered</CPEnt_Status>
        <CPEnt_TYPE>UEN</CPEnt_TYPE>
        <CPNonUEN_RegNo>NULL</CPNonUEN_RegNo>
        <CPNonUEN_Country>NULL</CPNonUEN_Country>
        <CPNonUEN_Name>NULL</CPNonUEN_Name>
</UserInfo>
```

Example Non-UEN CorpPass User Info XML – Decoded:

```
<UserInfo>
        <CPAccType>Admin</CPAccType>
        <CPUID>Z9239556A</CPUID>
        <CPUID_Country>CO</CPUID_Country>
        <CPUID_FullName>JUAN VALDEZ</CPUID_FullName>
        <CPSystemUID>CP25880</CPSystemUID>
        <ISSPHOLDER>NO</ISSPHOLDER>
        <CPEntID>C18000545L</CPEntID>
        <CPEnt_Status>NULL</CPEnt_Status>
        <CPEnt_TYPE>NON-UEN</CPEnt_TYPE>
        <CPNonUEN_RegNo>999999999</CPNonUEN_RegNo>
```

```
        <CPNonUEN_Country>CO</CPNonUEN_Country>
        <CPNonUEN_Name>JUAN VALDEZ</CPNonUEN_Name>
</UserInfo>
```

8.1.2 CorpPass User Authorization XML

This section provides the XML Schema (XSD) and example XML for CorpPass User Authorizations that will be shared from CorpPass IdP to the Digital Service as an attribute in SAML Assertion that is returned to Digital Service as part of CorpPass Authentication and Authorization.

Please note that this attribute will be mandatorily present in the assertion for all Digital Services using CorpPass, even if the Digital Service is using CorpPass for authentication only. If a Digital Service is using CorpPass for authentication only, the authorization XML will be NULL.

CorpPass User Authorization XSD:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
	<xs:element name="AuthAccess">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="Result_Set" maxOccurs="1" minOccurs="1">
					<xs:complexType>
						<xs:sequence>
							<xs:element type="xs:int" name="ESrvc_Row_Count" maxOccurs="1" minOccurs="1"/>
							<xs:element name="ESrvc_Result" maxOccurs="unbounded" minOccurs="1">
								<xs:complexType>
									<xs:sequence>
										<xs:element type="xs:string" name="CPESrvcID" maxOccurs="1" minOccurs="1"/>
										<xs:element name="Auth_Result_Set" maxOccurs="1" minOccurs="1">
	<xs:complexType>
	<xs:sequence>
	<xs:element type="xs:int" name="Row_Count" maxOccurs="1" minOccurs="1"/>
	<xs:element name="Row" maxOccurs="unbounded" minOccurs="1">
		<xs:complexType>
			<xs:sequence>
				<xs:element type="xs:string" name="CPEntID_SUB" maxOccurs="1" minOccurs="1"/>
				<xs:element type="xs:string" name="CPRole" maxOccurs="1" minOccurs="1"/>
```

```
                                    <xs:element type="xs:date" name="StartDate" maxOccurs="1" minOccurs="1"/>

                                    <xs:element type="xs:date" name="EndDate" maxOccurs="1" minOccurs="1"/>

                                    <xs:element name="Parameter" maxOccurs="8" minOccurs="0">

                                        <xs:complexType>

                                            <xs:simpleContent>

                                                <xs:extension base="xs:string">

                                                    <xs:attribute                type="xs:string"
name="name"/>

                                                </xs:extension>

                                            </xs:simpleContent>

                                        </xs:complexType>

                                    </xs:element>

                                </xs:sequence>

                            </xs:complexType>

                    </xs:element>

                    </xs:sequence>

                    </xs:complexType>
                                                                                    </xs:element>
                                                                                </xs:sequence>
                                                                            </xs:complexType>
                                                                        </xs:element>
                                                                    </xs:sequence>
                                                                </xs:complexType>
                                                            </xs:element>
                                                        </xs:sequence>
                                                    </xs:complexType>
                                            </xs:element>
</xs:schema>
```

Example CorpPass User Authorization XML – Base64 Encoded:

PEF1dGhBY2Nlc3M+DQoJPFJlc3VsdF9TZXQ+DQoJCTxFU3J2Y19Sb3dfQ291bnQ+MTwvRVNydmNfUm93X0NvdW50Pg
0KCQk8RVNydmNfUmVzdWx0Pg0KCQkJPENQRVNydmNJRD5CR0VTUlYxPC9DUEVTcnZjSUQ+DQoJCQk8QXV0aF9S
ZXN1bHRfU2V0Pg0KCQkJCTxSb3dfQ291bnQ+MjwvUm93X0NvdW50Pg0KCQkJCTxSb3c+DQoJCQkJCTxDUEVudElEX1
NVQj5OVUxMPC9DUEVudElEX1NVQj4NCgkJCQkJPENQUm9sZT5OVUxMPC9DUEVudElEX1NVQj4NCgkJCQkJCTxTdGFydERh
dGU+MjAxNi0wMS0xNTwvU3RhcnREYXRlPg0KCQkJCQkJCTxTdGFydERhdGU+MjAxNi0wMS0xNTwvU3RhcnREYXRlPg
0KCQkJCQkJCTxFbmREYXRlPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9IlllYXIgb2YgYXNzZXNzbWVudCI+MjAxNDwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDIiPnZhbHVlIDAyPC9QYXJhbWV0ZXI+DQoJCQkJCTxQYXJhbWV0ZXIgbmFtZT0ib3RoZXIgbmFtZT0iZXIwMyI+dmFsdWUgMDM8L1BhcmFtZXRlcj4NCgkJCQkJPFBhcmFtZXRlciBuYW1lPSJvdGhlcjA0Ij52YWx1ZSAwNDwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDUiPnZhbHVlIDA1PC9QYXJhbWV0ZXI+DQoJCQkJCTxQYXJhbWV0ZXIgbmFtZT0iZXIwNiI+dmFsdWUgMDY8L1BhcmFtZXRlcj4NCgkJCQkJPFBhcmFtZXRlciBuYW1lPSJvdGhlcjA3Ij52YWx1ZSAwNzwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDgiPnZhbHVlIDA4PC9QYXJhbWV0ZXI+DQoJCQkJPC9Sb3c+CQkJCTxSb3c+DQoJCQkJCTxDUEVudElEX1NVQj5OVUxMPC9DUEVudElEX1NVQj4NCgkJCQkJPENQUm9sZT5OVUxMPC9DUEVudElEX1NVQj4NCgkJCQkJCTxTdGFydERhdGU+MjAxNi0wMS0xNTwvU3RhcnREYXRlPg0KCQkJCQkJCTxTdGFydERhdGU+MjAxNi0wMS0xNTwvU3RhcnREYXRlPg0KCQkJCQkJCTxFbmREYXRlPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9IlllYXIgb2YgYXNzZXNzbWVudCI+MjAxNDwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDIiPnZhbHVlIDAyPC9QYXJhbWV0ZXI+DQoJCQkJCTxQYXJhbWV0ZXIgbmFtZT0ib3RoZXIgbmFtZT0iZXIwMyI+dmFsdWUgMDM8L1BhcmFtZXRlcj4NCgkJCQkJPFBhcmFtZXRlciBuYW1lPSJvdGhlcjA0Ij52YWx1ZSAwNDwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDUiPnZhbHVlIDA1PC9QYXJhbWV0ZXI+DQoJCQkJCTxQYXJhbWV0ZXIgbmFtZT0iZXIwNiI+dmFsdWUgMDY8L1BhcmFtZXRlcj4NCgkJCQkJPFBhcmFtZXRlciBuYW1lPSJvdGhlcjA3Ij52YWx1ZSAwNzwvUGFyYW1ldGVyPg0KCQkJCQk8UGFyYW1ldGVyIG5hbWU9Im90aGVyMDgiPnZhbHVlIDA4PC9QYXJhbWV0ZXI+DQoJCQkJPC9Sb3c+CQkJPC9BdXRoX1Jlc3VsdF9TZXQ+DQoJCTwvRVNydmNfUmVzdWx0Pg0KCTwvUmVzdWx0X1NldD4NCjwvQXV0aEFjY2Vzcz4=

Example CorpPass User Authorization XML – Decoded:

```
<AuthAccess>
	<Result_Set>
		<ESrvc_Row_Count>1</ESrvc_Row_Count>
		<ESrvc_Result>
			<CPESrvcID>BGESRV1</CPESrvcID>
			<Auth_Result_Set>
				<Row_Count>2</Row_Count>
				<Row>
					<CPEntID_SUB>NULL</CPEntID_SUB>
					<CPRole>NULL</CPRole>
					<StartDate>2016-01-15</StartDate>
					<EndDate>2016-02-15</EndDate>
				</Row>
				<Row>
					<CPEntID_SUB>NULL</CPEntID_SUB>
					<CPRole>NULL</CPRole>
					<StartDate>2016-03-15</StartDate>
					<EndDate>2017-04-15</EndDate>
					<Parameter name="Year of assessment">2014</Parameter>
					<Parameter name="other02">value 02</Parameter>
					<Parameter name="other03">value 03</Parameter>
					<Parameter name="other04">value 04</Parameter>
					<Parameter name="other05">value 05</Parameter>
					<Parameter name="other06">value 06</Parameter>
					<Parameter name="other07">value 07</Parameter>
					<Parameter name="other08">value 08</Parameter>
				</Row>
			</Auth_Result_Set>
		</ESrvc_Result>
	</Result_Set>
</AuthAccess>
```

8.1.3 CorpPass Third Party Authorization XML

For Digital Services that have Third Party functionality, if a third party user logs in to Digital Service using CorpPass, in addition to User Authorization XML, an additional Third Party Authorization XML will be shared as an additional attribute in SAML assertion. This section provides the XML schema (XSD) and example XML for Third Party Authorizations.

In Third Party authorizations, a user can have multiple authorizations for a Digital Service i.e. the third party can have multiple clients for which the user has authorizations for a given Digital Service.

E.g. For GST Digital Service, a third party entity may have 5 clients and a user in the third party entity can be entitled to file GST for all the 5 clients. This would mean that the user will have 5 third party authorizations for GST Digital Service.

To ensure that the user can transact on behalf of any of the clients in the Digital Service, when the user logs in using CorpPass, CorpPass IdP will share the authorizations for all the clients within the same XML (i.e. in the same attribute in assertion). This is to ensure that Digital Service can provide the user with the option to select the client entity ID that they want to transact for within the Digital Service without requiring additional calls to CorpPass IdP.

Please note that this <TPAuthAccess> element will added to existing <UserInfo> and <AuthAccess> elements in the assertion for all Digital Services using CorpPass in third-party scenario ONLY.

CorpPass Third Party Authorization XSD:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="TPAuthAccess">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="CP_TPEntID" type="xs:string" maxOccurs="1"
minOccurs="1"/>
                <xs:element name="CP_TPEnt_Status" type="xs:string" maxOccurs="1"
minOccurs="1"/>
                <xs:element name="CP_TPEnt_TYPE" type="xs:string" maxOccurs="1"
minOccurs="1"/>
                <xs:element name="Result_Set" maxOccurs="1" minOccurs="1">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="ESrvc_Row_Count"
type="xs:int" maxOccurs="1" minOccurs="1"/>
                            <xs:element name="ESrvc_Result"
maxOccurs="unbounded" minOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element
name="CPESrvcID" type="xs:string" maxOccurs="1" minOccurs="1"/>
```

```
                                                                    <xs:element
name="Auth_Set" maxOccurs="1" minOccurs="1">
        <xs:complexType>
        <xs:sequence>
        <xs:element name="ENT_ROW_COUNT" type="xs:int" maxOccurs="1" minOccurs="1"/>
        <xs:element name="TP_Auth" maxOccurs="unbounded" minOccurs="1">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="CP_Clnt_ID" type="xs:string" maxOccurs="1" minOccurs="1"/>
                                <xs:element      name="CP_ClntEnt_TYPE"      type="xs:string"      maxOccurs="1"
minOccurs="1"/>
                                <xs:element name="Auth_Result_Set" maxOccurs="1" minOccurs="1">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element      name="Row_Count"      type="xs:int"
maxOccurs="1" minOccurs="1"/>
                                                        <xs:element  name="Row"  maxOccurs="unbounded"
minOccurs="1">
                                                                <xs:complexType>
                                                                        <xs:sequence>
                                                                                <xs:element
name="CP_ClntEnt_SUB" type="xs:string" maxOccurs="1" minOccurs="1"/>
                                                                                <xs:element
name="CPRole" type="xs:string" maxOccurs="1" minOccurs="1"/>
                                                                                <xs:element
type="xs:date" name="StartDate"  maxOccurs="1" minOccurs="1"/>
                                                                                <xs:element
type="xs:date" name="EndDate"  maxOccurs="1" minOccurs="1"/>
                                                                                <xs:element
name="Parameter" maxOccurs="8" minOccurs="0">
```

```
<xs:complexType>

<xs:simpleContent>

<xs:extension base="xs:string">

        <xs:attribute type="xs:string" name="name"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>
                                                                    </xs:element>
                                                                </xs:sequence>
                                                            </xs:complexType>
                                                        </xs:element>
                                                    </xs:sequence>
                                                </xs:complexType>
                                            </xs:element>
                                        </xs:sequence>
                                    </xs:complexType>
</xs:element>

</xs:sequence>

</xs:complexType>
                                                                    </xs:element>
                                                                </xs:sequence>
                                                            </xs:complexType>
                                                        </xs:element>
```

```
                                                    </xs:sequence>
                                                </xs:complexType>
                                            </xs:element>
                                        </xs:sequence>
                                    </xs:complexType>
                                </xs:element>
</xs:schema>
```

Example CorpPass Third Party Authorization XML – Base64 Encoded:

PFRQQXV0aEFjY2Vzcz4NCgk8Q1BfVFBFbnRJRD43ODEyOTM4NFA8L0NQX1RQRW50SUQ+DQoJPENQX1RQRW50X
1N0YXR1cz5SZWdpc3RlcmVkPC9DUF9UUEVudF9TdGF0dXM+DQoJPENQX1RQRW50X1RZUEU+VUVOPC9DUF9UUE
VudF9UWVBFPg0KCTxSZXN1bHRfU2V0Pg0KCQk8RVNydmNfUm93X0NvdW50PjE8L0VTcnZjX1Jvd19Db3VudD4NCgkJ
PEVTcnZjX1Jlc3VsdD4NCgkJCTxDUEVTcnZjSUQ+SVJJJTi1FU1JWQzE8L0NQRVNydmNJRD4NCgkJCTxBdXRoX1NldD4
NCgkJCQk8RU5UX1JPV19DT1VOVD4yPC9FTlRfUk9XX0NPVU5UPg0KCQkJCTxUUF9BdXRoPg0KCQkJCQk8Q1BfQ2x
udF9JRD5UMTVVRjM1NjRGPC9DUF9DbG50X0lEPg0KCQkJCQk8Q1BfQ2xudEVudF9UWVBFPlVFTjwvQ1BfQ2xudEVud
F9UWVBFPg0KCQkJCQk8QXV0aF9SZXN1bHRfU2V0Pg0KCQkJCQkJPFJvd19Db3VudD4yPC9Sb3dfQ291bnQ+DQoJCQ
kJCQk8Um93Pg0KCQkJCQkJCTxDUF9DbG50RW50X1NVQj5NMTIzNDU2NzhYPC9DUF9DbG50RW50X1NVQj4NCgkJC
QkJCQk8Q1BSb2xlPk5VTEw8L0NQUm9sZT4NCgkJCQkJCQk8U3RhcnREEYXRlPjIwMTEtMDEtMTU8L1N0YXJ0RGF0ZT4
NCgkJCQkJCQk8RW5kRGF0ZT4yMDExLTAxLTE1PC9FbmREEYXRlPg0KCQkJCQkJCTxQYXJhbWV0ZXIgbmFtZT0iWWV
hciBvZiBhc3Nlc3NtZW50Ij4yMDE1PC9QYXJhbWV0ZXI+DQoJCQkJCQk8L1Jvdz4NCgkJCQkJCTxSb3c+DQoJCQkJ
PENQX0NsbnRFbnRfU1VCPk0xOTk0NTY3OFg8L0NQX0NsbnRFbnRfU1VCPg0KCQkJCQkJCTxDUFJvbGU+QXBwcm92
ZXI8L0NQUm9sZT4NCgkJCQkJCQk8U3RhcnREEYXRlPjIwMTEtMDEtMTU8L1N0YXJ0RGF0ZT4NCgkJCQkJCQk8RW5kR
GF0ZT4yMDExLTAxLTE1PC9FbmREEYXRlPg0KCQkJCQkJCTxQYXJhbWV0ZXIgbmFtZT0iWWVhciBvZiBhc3Nlc3NtZW50Ii
j4yMDE0PC9QYXJhbWV0ZXI+DQoJCQkJCQk8L1Jvdz4NCgkJCQkJPC9BdXRoX1Jlc3VsdF9TZXQ+DQoJCQkJPC9UUF9
BdXRoPg0KCQkJCTxUUF9BdXRoPg0KCQkJCQk8Q1BfQ2xudF9JRD4xOTkyMDYwMzFXPC9DUF9DbG50X0lEPg0KCQk
JCQk8Q1BfQ2xudEVudF9UWVBFPlVFTjwvQ1BfQ2xudEVudF9UWVBFPg0KCQkJCQk8QXV0aF9SZXN1bHRfU2V0Pg0K
CQkJCQkJPFJvd19Db3VudD4xPC9Sb3dfQ291bnQ+DQoJCQkJCQk8Um93Pg0KCQkJCQkJCTxDUF9DbG50RW50X1NV
Qj5NMTIzMDA2NzhBPC9DUF9DbG50RW50X1NVQj4NCgkJCQkJCQk8Q1BSb2xlPlByZXBhcmVyPC9DUFJvbGU+DQoJC
QkJCQkJPFN0YXJ0RGF0ZT4yMDExLTAxLTE1PC9TdGFydERhdGU+DQoJCQkJCQkJPEVuZERhdGU+MjAxMS0wMS0x
NTwvRW5kRGF0ZT4NCgkJCQkJCQk8UGFyYW1ldGVyIG5hbWU9IlllYXIgb2YgYXNzZXNzbWVudCI+MjAxNDwvUGFyYW
1ldGVyPg0KCQkJCQkJPC9Sb3c+DQoJCQkJCTwvQXV0aF9SZXN1bHRfU2V0Pg0KCQkJCTwvVFBfQXV0aD4NCgkJCTw
vQXV0aF9TZXQ+DQoJCTwvRVNydmNfUmVzdWx0Pg0KCTwvUmVzdWx0X1NldD4NCjwvVFBBdXRoQWNjZXNzPg==

Example CorpPass Third Party Authorization XML – Decoded:

```
<TPAuthAccess>
        <CP_TPEntID>78129384P</CP_TPEntID>
        <CP_TPEnt_Status>Registered</CP_TPEnt_Status>
        <CP_TPEnt_TYPE>UEN</CP_TPEnt_TYPE>
        <Result_Set>
                <ESrvc_Row_Count>1</ESrvc_Row_Count>
                <ESrvc_Result>
                        <CPESrvcID>IRIN-ESRVC1</CPESrvcID>
                        <Auth_Set>
                                <ENT_ROW_COUNT>2</ENT_ROW_COUNT>
                                <TP_Auth>
                                        <CP_Clnt_ID>T15UF3564F</CP_Clnt_ID>
                                        <CP_ClntEnt_TYPE>UEN</CP_ClntEnt_TYPE>
                                        <Auth_Result_Set>
                                                <Row_Count>2</Row_Count>
                                                <Row>

        <CP_ClntEnt_SUB>M12345678X</CP_ClntEnt_SUB>
                                                        <CPRole>NULL</CPRole>
                                                        <StartDate>2011-01-15</StartDate>
                                                        <EndDate>2011-01-15</EndDate>
                                                        <Parameter name="Year of
assessment">2015</Parameter>
                                                </Row>
                                                <Row>

        <CP_ClntEnt_SUB>M19945678X</CP_ClntEnt_SUB>
                                                        <CPRole>Approver</CPRole>
                                                        <StartDate>2011-01-15</StartDate>
                                                        <EndDate>2011-01-15</EndDate>
                                                        <Parameter name="Year of
assessment">2014</Parameter>
                                                </Row>
                                        </Auth_Result_Set>
                                </TP_Auth>
                                <TP_Auth>
                                        <CP_Clnt_ID>199206031W</CP_Clnt_ID>
                                        <CP_ClntEnt_TYPE>UEN</CP_ClntEnt_TYPE>
                                        <Auth_Result_Set>
                                                <Row_Count>1</Row_Count>
                                                <Row>

        <CP_ClntEnt_SUB>M12300678A</CP_ClntEnt_SUB>
                                                        <CPRole>Preparer</CPRole>
                                                        <StartDate>2011-01-15</StartDate>
                                                        <EndDate>2011-01-15</EndDate>
                                                        <Parameter name="Year of
assessment">2014</Parameter>
```

```
                                                    </Row>
                                                </Auth_Result_Set>
                                            </TP_Auth>
                                        </Auth_Set>
                                    </ESrvc_Result>
                                </Result_Set>
</TPAuthAccess>
```

9. ANNEXURE C

9.1 LOGIN REDIRECT URL TO IDP

Agencies need to implement a redirect URL from their Digital Service applications to IdP so that the user can come to IdP site. Once the user accesses the IdP site, IdP will initiate the SAML login flow provided Section 4.4.

Agencies need to update their Digital Service application to implement the redirect URL on the 'Login with CorpPass' button. As per SAML specification the format of the redirect URL should be as shown below.

Redirect URL Format:
<IDP Login URL>?RequestBinding=HTTPArtifact&ResponseBinding=HTTPArtifact&PartnerId=<SP SOAP End Point URL>&Target=<Digital Service Application Landing Page URL>&NameIdFormat=Email&esrvcID=<Digital Service ID>

Redirect URL Example:
https://saml.corppass.gov.sg/FIM/sps/CorpIDPFed/saml20/logininitial?RequestBinding=HTTPArtifact&ResponseBinding=HTTPArtifact&PartnerId=https://saml.agency.gov.sg/FIM/sps/SP01Fed/saml20&Target=https://eservice.agency.gov.sg/index.html& NameIdFormat=Email&esrvcID=e123

Redirect URL Parameter Description (Please note the following Parameter Name and values are case-sentitive):

Parameter Name	Parameter Description	Value
IDP Login URL	This URL refers the IDP Login page where the user is redirected to for authentication. This URL will be provided by SPCP project as part of the transition checklist for use by agencies	Example: https://saml.corppass.gov.sg/FIM/sps/IDP01Fed/saml20/logininitial
RequestBinding	This parameter refers to the binding protocol used for SAML requests. This should **always** be set to "**HTTPArtifact**"	**HTTPArtifact**
ResponseBinding	This parameter refers to the binding protocol used for SAML responses. This should **always** be set to "**HTTPArtifact**"	**HTTPArtifact**
PartnerId	This URL refers the SOAP end point URL that is setup in the Service Provider Module at the agency side. SOAP End Point is used for out-of-band (back	Example: https://saml.agency.gov.sg/FIM/sps/SP01Fed/saml20

	channel) communication for exchange of SAML assertions. Please note that this parameter needs to be URL encoded before embedding into the redirection. This URL needs to be provided as part of the metadata exchanged by the agencies after they complete the setup of their Service Provider.	Note: This parameter needs to be URL encoded. The example provided is not URL encoded to ensure readability.
Target	This URL refers to the URL of the Digital Service landing page where the user needs to be returned after the user completes the authentication process with IdP. Please note that this parameter needs to be URL encoded before embedding into the redirection. The URL will be specific to the Digital Service for which the user is authenticating.	Example: https://eservice.agency.gov.sg/index.html Note: This parameter needs to be URL encoded. The example provided is not URL encoded to ensure readability.
NameIdFormat	This parameter refers the format of the User ID that is passed back to agency Service Provider as part of the assertion. The formats used that can be used are defined as part of the SAML specification. For SPCP project this parameter will **always** have value set to '**Email**'. Email format allows exchange of NRIC/FIN as the user ID.	**Email**
esrvcID	This parameter contains the Digital Service ID for the Digital Service that is requesting authentication. Digital Service ID is provided by SPCP team when registering/onboarding a Digital Service to CorpPass	**Digital Service ID** Note: This value is provided by SPCP team during onboarding of Digital Service
param1	This parameter is for future use and is not used in the current implementation. The value for this parameter is **always** set to **NULL** (use the exact string value)	**NULL**
param2	This parameter is for future use and is not used in the current implementation. The value for this parameter is **always** set to **NULL** (use the exact string value)	**NULL**

9.2 USER'S 'CANCEL' SCENARIO

Agencies need to handle the 'cancel' scenario highlighted in SAML login flow under Section 4.4. CorpPass step 5a. CorpPass provides an option where user can click on the 'Cancel' button if he/she decided not to proceed to login with CorpPass.

When user clicks on the 'Cancel', CorpPass would redirect the user back to SP with the following two approaches:

1. "Referer URL" will be used if its found in the HTTP request headers.
2. "Target" parameter if the "Referer URL" is not found.
3. A "errorcode=CorpPass_00_00_01" HTTP request parameter will be appended for the redirection. Agency can use the errorcode in the parameter for further processing (if required).

Redirect URL Format:

1. <Referer URL>&errorcode=CorpPass_00_00_01; or
2. <Target paramater>&errorcode=CorpPass_00_00_01

Redirect URL Example:

1. https://www.agency.gov.sg/index.asp?param1=123&errorcode=CorpPass_00_00_01; or
2. https://eservice.agency.gov.sg/index.html?param1=123&errorcode=CorpPass_00_00_01

10. ANNEXURE D

10.1 AUTHENTICATION CONTEXT FOR 2FA LOGIN

As described above, CorpPass is the Identity Provider to provide user authentications and authorisations information to the service providers in the SAML assertion exchanged using back channel. The assertion contains the details of the user and their authorisations as well as the authentication mechanism used by the user during login (i.e. 1FA or 2FA).

The authentication mechanism details are in the Authentication Context (saml:AuthnContext) tag in the assertion. This section describes the AuthnContextClassRef values that will be included in assertion by CorpPass IdP for various types of authentication mechanisms.

10.1.1 One-factor Authentication (1FA)

1FA refers to authentication using 'Password'. In CorpPass, a user authenticates with CorpPass IdP using password presented over a secure HTTP session (HTTPS), therefore the authentication mechanism used is 'Password'.

URI: **urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport**

The PasswordProtectedTransport class is used when a user authenticates through the presentation of a password over a protected session.

The example assertion below shows part of the assertion (AuthnStatement) which contains the AuthnContext with the AuthnContextClassRef that provides the authentication mechanism details.

```
<saml:Assertion
  … … …
  <saml:AuthnStatement
   AuthnInstant="2004-12-05T09:22:00"
   SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
   <saml:AuthnContext>
    <saml:AuthnContextClassRef>
     urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
   </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

10.1.2 Two-factor Authentication (2FA) using Hardware Token

2FA using Hardware token refers to authentication using an OTP from generated by a token. In CorpPass, for Digital Services that require 2FA authentication a user can authenticate using token based OTP after completing 1FA. In this case the authentication mechanism used is 'TimeSyncToken'.

URI: **urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken**

The TimeSyncToken class is used when a user authenticates through a time synchronization token (hardware token).

The example assertion below shows part of the assertion (AuthnStatement) which contains the AuthnContext with the AuthnContextClassRef that provides the authentication mechanism details.

```
<saml:Assertion
  … … …
  <saml:AuthnStatement
   AuthnInstant="2004-12-05T09:22:00"
   SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
   <saml:AuthnContext>
    <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
    </saml:AuthnContextClassRef>
   </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

10.1.3 Two-factor Authentication (2FA) using Mobile SMS OTP

2FA using Mobile SMS OTP refers to authentication using an OTP sent to the user's mobile through SMS. In CorpPass, for Digital Services that require 2FA authentication a user can authenticate using Mobile SMS OTP after completing 1FA. In this case the authentication mechanism used is 'MobileTwoFactorUnregistered'.

URI: **urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered**

The MobileTwoFactorUnregistered is used when a user authenticates for 2FA using a mobile supplied two-factor.

The example assertion below shows part of the assertion (AuthnStatement) which contains the AuthnContext with the AuthnContextClassRef that provides the authentication mechanism details.

```
<saml:Assertion
  … … …
  <saml:AuthnStatement
   AuthnInstant="2004-12-05T09:22:00"
   SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
   <saml:AuthnContext>
```

```
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

10.1.4 Two-factor Authentication (2FA) using CorpPass Soft Token

2FA using CorpPass Soft Token refers to authentication using a mobile application sent to the user's mobile through push notification. In CorpPass, for Digital Services that require 2FA authentication in two scenarios:

- a SingPass-backed user can authenticate using SingPass Soft Token after completing 1FA. In this case the authentication mechanism used is '**SoftwarePKI**'.
- a CorpPass Foreign user can authenticate using CorpPass Soft Token after completing 1FA. In this case the authentication mechanism used is '**SoftwarePKI**'

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:**SoftwarePKI**

The **SoftwarePKI** is used when a user authenticates for 2FA using a mobile application supplied two-factor through push notification.

The example assertion below shows part of the assertion (AuthnStatement) which contains the AuthnContext with the AuthnContextClassRef that provides the authentication mechanism details.

```
<saml:Assertion
  … … …
  <saml:AuthnStatement
    AuthnInstant="2004-12-05T09:22:00"
    SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

11. ANNEXURE E

11.1 USER TYPES & AUTHORIZATION MATRIX

Refer to next page.

User – Type	XML Payload	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Scenario 6	Scenario 7
Golden Profile (GP)	• UserInfo contains: ○ Entity information; and • AuthAccess contains: ○ Default role	●			●		●	●
Explicit Assignment	• UserInfo contains: ○ Entity Information; and • AuthAccess contains: ○ [Sub-UEN, or ○ Assigned role, or ○ Agency's specific parameters]		●		● (Overwrite GP)	●		● (Overwrite GP)
3rd Party user	• UserInfo contains: ○ Entity information; and • AuthAccess contains: ○ [Sub-UEN, or ○ Assigned role, or ○ Agency's specific parameters]; and • TPAuthAccess contains: ○ Entity information; and ○ [3rd-Party Entity information; or ○ 3rd-Party Sub-UEN; or ○ 3rd-Party Role; or ○ 3rd-Party Agency's specific parameters]			●		●	●	●
Resultant Authorisation		<UserInfo> <AuthAccess>	<UserInfo> <AuthAccess>	<UserInfo> **<AuthAccess with NULL values>** <TPAuthAccess>	<UserInfo> <AuthAccess>	<UserInfo> <AuthAccess> <TPAuthAccess>	<UserInfo> <AuthAccess> <TPAuthAccess>	<UserInfo> <AuthAccess> <TPAuthAccess>