

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

1. Version History

Version	Date	Status	Author	Changes
1.0	2/9/2015	Proposal	J Randall	Initial version
1.1	9/10/2015	Signed off	J Randall	Minor update to scopes
1.2	26/10/2015	Proposal	J Randall	Renamed. Documented clients, added scope for server applications, added support for third parties. Also removed section on migration as this is no longer relevant.
1.3	25/1/2016	Proposal	J Randall	Added claim for underlying provider and third party vendor ID. Corrected authorization code flows to client credential flows. Updated section on refreshing tokens and added a section on long lived sessions. Added detail on user impersonation within machine to machine scenario.
1.4	25/1/2016	Proposal	J Randall	Corrected claims for simsserverapplication
1.5	26/1/2016	Proposal	J Randall	Removed schoolidentifiers from simsserverapplication, added name claim
2.0.0	16/2/2016	Proposal	J Randall	Adopted semantic versioning, added breaking changes to claims key change being replacement of simsschoolidentifier and simsschoolidentifiers with the new organisation claims. Removed onboarding workflows and other supporting text and made the spec more about SIMS as a whole than Satellites. Added section on identity providers.
2.0.1	31/3/2016	Signed off	J Randall	Incorporated feedback provided on 2.0.1.
3.0.0	15/9/2016	Proposal	A Smith	Renamed any references of Third Party to Partner Management related terms. Updated Partner Managemet related

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016


				scopes and claim names to reflect Partner Management branding. Explicitly added optional offline_access scope to hybrid security flows which will allow refresh tokens to be granted.
3.0.1	07/11/2016	Proposal	M Wilson	Update following meetings and integrator requirements updates to Clients list and scopes
3.0.2	23/11/2016	Proposal	M Wilson	Token content agreement meeting, added depreciated token values for completeness. Added Consent section. Renamed identifiers to be more generic providing common use cases outside of scenario specific. Updated "school" to be "organisation".
3.0.3	29/11/2016	Proposal	M Wilson	Correction regarding simsapplication and simsapplicationserver clients and † moved to the corresponding scopes
3.0.4	02/12/2016	Proposal	M Wilson	Updated Token Structure section to explicitly define the sub differencefor the authentication flow. Corrected PM identifiers
3.0.4	16/12/2016	Signed Off	Mike Smith	Feedback incorportade and issue as final approved version

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

2. Introduction

The next generation of SIMS projects make use of an interoperable service architecture exposed to the customer as a series of web and mobile applications that make use of a variety of services.

Access to these services is gated by a Security Token Service that implements the Open ID Connect¹ protocol and the remainder of this document assumes basic familiarity with that protocol and modern web security concepts. Partner access to the service layer via Partner Management APIs is also gated by the same Security Token Service.

This document outlines the scopes and claims used in this process and how the STS supports the key scenarios required. Deprecatead scopes and/or claims will have be indicated with a Y in the column headed with .

The current STS implementation is based on IdentityServer3 and is hosted in the live environment at <https://sts.sims.co.uk>.

3. Clients

The following clients are defined for use by applications:

Client	Auth Flow	Available Scopes	Description
simsapplication	Hybrid	openid* registration simsapplication† simsmultischoolapplication† parent student staff offline_access ²	Capita SIMS applications requiring a user context utilize the client to retrieve tokens compatible with the public API. Redirect URIs are restricted to Capita SIMS applications.
sa-{guid}	Hybrid	openid* registration simsapplication† simsmultischoolapplication† parent	Capita SIMS applications requiring a user context utilize the client to

¹ <http://openid.net/connect/>

² http://openid.net/specs/openid-connect-core-1_0.html#OfflineAccess requests with the offline_access scope will return a refresh token - used primarily with mobile apps.

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

		student staff offline_access ³	retrieve tokens compatible with the public API. Redirect URIs are restricted to Capita SIMS applications.
simsapplicationserver	Client Credential	openid* simsserverapplication*	Used for Capita SIMS authored customer applicaton supporting background services.
sas-{guid} (Sims Application Server)	Client Credential	openid*	Used for Capita SIMS authored customer application supporting background services that require a user context.
ssm-{guid}	Client Credential	openid* ssm-read ssm-write	Used by the SIMS Service Manager package for reading / writing cloud data.
pm-{guid}	Hybrid	openid* simsapplication+ simsmultischoolapplication+ partner* offline_access	Used for Partner Management - Partner applications requiring a user context utilize the client to

³ http://openid.net/specs/openid-connect-core-1_0.html#OfflineAccess requests with the offline_access scope will return a refresh token - used primarily with mobile apps.

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

			<p>retrieve tokens compatible with the public API.</p> <p>Redirect URIs are restricted to those registered by our partners and the URI can be used in conjunction with the client ID (supplied in the hybrid flow) to establish the vendor ID.</p>
pms-{guid} (Partner Management Application Server)	Client Credential	openid* simsserverapplication partner*	Used Partner management - Partner applications supporting background services.

Notes:

Scopes marked with a * are required and must be requested when using the associated client.

The scopes marked with † cannot be used by a single client. The application should be clearly defined and work in only one of the application modes.

Finally note that the openid scope is always required. While many identity providers will function without this scope the Open ID Connect Specification makes no guarantees over identity provider behavior if it is not requested (and in fact warns of not including this)⁴.

Clients with the –{guid} postfix have multiple instances as follows:

Client	Instance Model
sa-{guid}	Per application.
sas-{guid}	Per school. Client appears in school admin / SIMS 8 and the school is able to assign a user the client acts on behalf of.
ssm-{guid}	Per school. Generated during onboarding.

⁴ See http://openid.net/specs/openid-connect-core-1_0.html#Authentication for details of configuration for the different authentication flows.

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

pm-{guid}	Per Partner Management - Partner application.
pms-{guid}	Per Partner Management - Partner application server.
pmdev-{guid}	Per Partner Management - Partner applications that are in development.
pmsdev-{guid}	Per Partner Management - Partner application server that are in development.

3.1 Clients Consent


Clients that are identified as Capita produced and owned do not have explicitly have consent granted for accessing the Users information.

Partner application consent is managed by the Partner Management API interface and as such consent screens will not be shown.

Any client falling outside of the Capita or Partner client space will be required to show a consent screen.

4. Scopes

The following scopes are defined for use by applications:

Scope	Description	
registration	Required to access services involved in the system and user onboarding processes. This scope can be obtained by users who have authenticated with an identity provider but are not yet known as a SIMS user ⁵ .	
simsapplication†	<p>Required to access a single organisation focused SIMS application. See 5.2. This scope can only be obtained by users who have authenticated with an identity provider and are known as a SIMS user.</p> <p>The application can understand multiple organisations and can translate the single organisation into an organisation structure for use in the application.</p> <p>When a user signs into an application but is known to be associated with multiple schools the STS is expected to offer them a choice of school and populate the userorganisationidentifier claim appropriately.</p>	

⁵ Being known as a SIMS user is defined as the STS having a school ID and SIMS user ID (SIMS external ID) associated with their identity provider subject.

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

simsmultischoolapplication†	Required to access multiple organisations in an unstructured way, or where there is no relationship between the organisations required for the application to function. Required to access a multiple organisation focused SIMS Satellite application. See 5.2.	Y
simsmultiorgapplication†	Required to access multiple organisations in an unstructured way, or where there is no relationship between the organisations required for the application to function. Required to access a multiple organisation focused SIMS Satellite application. See 5.2.	
simsserverapplication	Required in non-interactive authentication and authorization scenarios such as background processing within worker roles typically where a server has been asked to undertake lengthy tasks on behalf of a user in an implied trust scenario..	
capitaserverapplication	Used by Capita internal services (e.g. a CRM daemon) in non-interactive authentication and authorization scenarios. Some back end systems require a differentiation between a customer focused application and an internal application and this scope provides that.	
ssm-read	Required by the SIMS Services Manager package to read data from the cloud.	
ssm-write	Required by the SIMS Services Manager package to write / upload data to the cloud.	
openid	One of the standard Open ID Connect scopes and required to obtain an id_token to support key pieces of IdentityServer3 functionality such as auto-redirect after logout.	
sims7{area}	It is anticipated that we will create multiple scopes in this format. later in this document for more details.	
parent	If requested by a relying party it signifies the relying party is primarily used by parents.	
student	If requested by a relying party it signifies the relying party is primarily used by students.	
staff	If requested by a relying party it signifies the relying party	

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016


	is primarily used by staff.	
partner-application	Required to access a single organisation focused Partner application. See 5.2. This scope can only be obtained by users who have authenticated with an identity provider and are known as a SIMS user. The application can understand multiple organisations and can translate the single organisation into an organisation structure for use in the application.	
offline_access	Used by a requesting client to request a Refresh Token.	

The scopes marked with † cannot be used by a single client. The application should be clearly defined and work in only one of the application modes.

The parent, student and staff scopes are primarily intended to allow the logon page to adopt the most appropriate branding to be presented based on the destination relying party.

5. Claims

The following claims are issued by the STS dependent on the scopes requested.

Claim	Scopes	Description	
userorganisationidentifier	simapplication partner application ssm-read ssm-write	Identifies the user and organisation that a user is considered to be logged into as a primary school. Typically used by applications that are focused on single school / organization interactions such as SIMS Activities Organizer. Typically these applications are for use by school staff. There will only be a single value associated with this claim. See 5.1 below for details on how this claim is constructed.	

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

userorganisationidentifiers	simsmultischoolapplication simsmultiorgapplication	<p>Identifies the set of organisations that a user is associated with and their SIMS external ID within each organisation. Typically used by applications that are focused on interactions across small numbers of multiple organisations such as the SIMS Parent app where a parent is likely to have children at multiple organisations and wishes to view data from them in a joined up fashion.</p> <p>There can be multiple values associated with this claim. Each value takes the same format as the userorganisationidentifier claim.</p> <p>The resulting array of claims will be limited to 10. If the user has access to more than 10 organisations then the calling application can query SIMS ID to retrieve the full organization list.</p>	
partnerapplicationid	Partner application	<p>The ID of the Partner application that retrieved the token.</p> <p>e.g. SIMS Primary application</p>	Y
applicationid	simssapplication simsmultischoolapplication simsmultiorgapplication	The ID of the application that retrieved the token.	

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

	simsserverapplication capitaserverapplication partner application		
partnervendorid	partner application	The ID of the Partner as known to the Partner Management APIs. e.g for SIMS Primary this would CCS.	Y
vendorid	simsapplication simsmultischoolapplication simsmultiorgapplication simsserverapplication capitaserverapplication partner	The ID of the vendor. For Capita authored applications this will be the vendor id for Capita. Partners will be identified by their ID as known to the Partner Management APIs.	
idp	All scopes	The underlying identity provider as supplied by the identity provider itself.	
name	simsapplication simsmultischoolapplication	Name of the user	
launcher	All Scopes	Used by SIMS ID applications	Y
Site	All Scopes	Contains the Organisations identifier code. For schools this is their DfE Code, for other Organisations this is a unique defined code a a maximum of 8 chars in length.	Y
homeorganisationidentifier	All Scopes	Used by SIMS Primary to identify the home organization of the User as configured in SIMS ID	Y
multipleorganisations	All Scopes	Boolean value that is used to identify if the User is a member of	

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

		multiple	
provider	All Scopes	Identifies the identity provider	
providerid	All Scopes	The Users identifier for the provider	

As access tokens are communicated in the Authorization header of every service call and the system is expected to be heavily used over mobile networks then care needs to be taken to keep the size small and therefore additional claims should only be added with due consideration.

Where data is not available the claim will be blank. Thought needs to be given to audited entries.

5.1 userorganisationidentifier and userorganisationidentifiers Claims

These claims identify a user at an organization and the type of that organization. To prevent issues with misaligned arrays the claims take a compound format as shown below:

```
{userid}|{organisationid}|{organisationtype}
```

The component parts are as follows:

Component	Type	Description
userid	Guid	The ID of the user as understood by all Capita and Partner Management systems (the SIMS External ID).
organisationid	Guid	The ID of the organisation as determined by the School & Enterprise Service ⁶ .
organisationtype	String	A string that contain multiple characters with each character in the sequence representing an organization type as described below.

Organisations can be of the following types; the definition and maintenance of the organisation codes rests with the ODS service:

Code	Meaning
C	Capita
G	School Group
L	Local Authority
M	Multi Academy Trust

⁶ In advance of the School & Enterprise Service being available this ID is sourced from the CRM system.

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

O	Support Organisation
S	School

5.1.1 Examples

The following sequence represents a user (c498...) at organization (a87b...) that is a School:

c498dcbc-6832-4872-bbd3-1cc7072c57d5|a87b917e-9e52-440e-aebc-f48de5463597|S

The following sequence represents a user (a9ab...) at organization (99af...) that is a Multi Academy Trust:

a9abb2ca-342c-4bdd-94b7-cc6c4a98c6de|99af4670-8ad6-473d-97cb-79b396255c16|M

The following sequence represents a user (...) at organization (...) that is both a Multi Academy Trust and a School:

8aad423b-4058-4a45-b06c-8dc8e72de5a0|88fedc13-3a68-4ea1-94fb-053f8abafe88|MS

5.2 Single and Multi School Application Models

We already have examples of applications that present and interact with data from multiple schools simultaneously – examples being the SIMS Parent app and Extra Curricular parent website. We also have examples which focus on a single schools data – examples being the School Admin and Extra Curricular Organiser websites.

It is expected that users will be able to navigate between these applications and the userorganisationidentifier and userorganisationidentifiers claims support these models.

The userorganisationidentifier is set by an initial decision on entry to a single application model (where a user has rights to multiple schools in that model) and can be reset through the claim refresh mechanism.

5.3 Refreshing Claims

During a session the access_token will occasionally require refreshing in order to obtain the latest set of claims. The two scenarios currently identified where this is required are:

1. During the system onboarding process when a user maps themselves from a temporary user to a real user (see System Onboarding).
2. When a user changes school in a multi-school application.

Two approaches are required for this depending on the scenario.

5.3.1 Native Application

In order to support this the application must be using the IdentityServer3 hybrid authentication flow and have obtained a refresh token. The application can then use the token endpoint with the refresh token to generate a new access token containing the latest claims.

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

5.3.2 *Web (SPA) Application*

A single page web application should not hold on to a refresh token and therefore should use the silent token refresh approach using an invisible iframe to contact the token endpoint and specifying a prompt of none⁷.

5.4 Long Lived Sessions

Access tokens should have short lifetimes however this can impair the user experience if users are required to frequently log in. One of the following approaches should be adopted for obtaining a new access token and transparently extending a session.

5.4.1 *Native Application*

A native application should obtain a refresh token that it can then use with the token endpoint to generate a new access token on expiry of that token.

5.4.2 *Web (SPA) Application*

A single page web application should use the silent token refresh approach to obtain a new access token shortly (2 minutes typically) before the access token is due to expire.

6. Identity Providers

6.1 Required Identity Sources

Any token provider is required to support the following minimum set of identity providers.

- Azure AD / Office 365
- Facebook
- Google
- Microsoft Account
- SIMS ID
- Twitter

6.2 Identity Provider Restriction by Audience

From the School Admin system the school is able to restrict the identity providers that a given user / category of user can use. For example they may choose to enforce that school staff must use Office 365 accounts on a specific domain whereas Parents and Students may use any identity provider.

7. Restrictions on Clients

A small number of restrictions are placed on clients retrieving tokens from the STS.

⁷ A worked example for this can be found in the code for the AngularJS-OAuth2 plugin <https://github.com/JamesRandall/AngularJS-OAuth2/blob/master/dist/angularJsOAuth2.js#L211>

SIMS	Version: 3.0.4
Open ID Connect Configuration	Date: 16/12/2016

1. The HTTPS protocol must be used for all communication. The STS should reject redirect URIs that do not use this protocol and any incoming requests that do not use this protocol.
2. When deployed in the live environment (as opposed to the instance used in the development environment) the STS should reject localhost based redirect URIs with a single exception: partner application using specific Partner Clients that are specifically for use with the test SIMS 8 instances (see Partner API team and programme). Test clients will have a specific GUID naming convention of pmdev-guid & pmsdev-guid

8. Token Structure

The token structure as defined in [JSON Web Token \(JWT\) Profile for OAuth 2.0 Client Authentication and Authorization Grants Section 3.2](#) requires the sub claim to be defined differently depending on grant type.

8.1 Authorisation Grant Type

Down stream auditing depends on the sub claim. This MUST only be the SIMS ID immutable id. For backwards compatibility the current subject claim will be deprecated in its current format of {ImmutableID}|{GUID}|{UPN}|{Provider} to be {ImmutableID}.

This depreciation will be completed by the end of Q1 2017. Consuming applications that rely on these pipe separated values are encouraged to migrate to the replacement claims.

9. Multi-factor Authentication

Implementation of multi-factor authentication is the responsibility of the underlying identity provider in use and any configuration of that the responsibility of the customer.