Queensland Government Enterprise Architecture

Federated identity blueprint

Standards

Final

May 2017

V1.0.0

PUBLIC

Document details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Security classification** | 1. PUBLIC | | | | | |
| 1. **Date of review of security classification** | 1. May 2017 | | | | | |
| 1. **Authority** | 1. Queensland Government Chief Information Officer | | | | | |
| 1. **Author** | 1. Queensland Government Chief Information Office | | | | | |
| 1. **Documentation status** |  | 1. Working draft |  | 1. Consultation release | 1. 🗹 | 1. Final version |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Chief Information Office  
[qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au)

Acknowledgements

This version of the *Federated identity blueprint - Standards* was developed and updated Queensland Government Chief Information Office.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

*Federated identity blueprint - Standards*

Copyright © The State of Queensland (Queensland Government Chief Information Office) 2017

Licence

[](http://creativecommons.org/licenses/by/4.0/)

This work is licensed under a Creative Commons Attribution 4.0 International licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. For permissions beyond the scope of this licence, contact [qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au).

To attribute this material, cite the Queensland Government Chief Information Office.

The licence does not apply to any branding or images.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1 Standards 4](#_Toc484422477)

[1.1 Providers of credential, identity and attributes 4](#_Toc484422478)

[1.2 Relying parties 10](#_Toc484422479)

[1.3 Federation schemes 12](#_Toc484422480)

[1.4 Identity federation protocols 13](#_Toc484422481)

[Appendix A Standard versions 16](#_Toc484422482)

# Standards

## Providers of credential, identity and attributes

| Element | Requirements |
| --- | --- |
| **All Identity Providers** | The following requirements apply to all Queensland Government identity and credential providers:   |  |  | | --- | --- | | *Federation metadata publishing* | Identity Providers are required to publish (or make available) appropriate federation metadata compliant with relevant federation protocol standards supported to streamline configuration of federations. | | *Network time synchronisation* | Authentication services should synchronise time from an appropriate stratum service in accordance with the Queensland Government Network Time Protocol (NTP) architecture to minimise the risk of clock skew impacting authentication events. This is of particular importance for QGSFAS for agencies using the Hosted IdP (Kerberos) option. | | *Certificate & Key Management for Token Transport Security, Token Signing or Token Encryption* | Public-key infrastructure (PKI) is an important consideration for federation as it extends a fabric of trust across boundaries.  The appropriate CA to use will vary for a given trust relationship. Private CA’s may provide for stronger assurance over enrolment which may be more important than the convince of public CA’s. The CA may be the IdP itself or a well-known commercial CA. | | *Security & Privacy Compliance* | Polices regarding operation of Queensland Government Identity and Credential Providers (e.g. requirements for audit, security penetration testing, privacy impact assessments etc.) are to be developed under the Identity Policy IDC. |   Support for the following identity protocols are applicable as indicated below:  **SAML IdP**   |  |  | | --- | --- | | SSO Profiles | Applicability | | *Web browser profile* | Most common to support SSO. See decision framework - Determine authentication protocol flow | | *Enhanced client or Proxy (ECP) profile* | As required. See decision framework – Assertion security | | *Identity provider discovery profile* | If federation service required (see decision framework). Although most implementations are proprietary. | | *Single logout profile* | As required based on session management strategy (see decision framework) | | *Assertion query/request profiles* | Very specific use cases |   **OpenID Connect (OIDC) Provider**   |  |  | | --- | --- | | Core Flows | Applicability | | *Authorisation code* | Covers most common user cases and application clients | | *Implicit* | Covers most common use cases and application clients | | *Hybrid* | Most common to support SSO. See decision framework - Determine authentication protocol flow | | *Discovery* | As required. See decision framework – Assertion security | | *Dynamic registration* | If federation service required (see decision framework). Although most implementations are proprietary. | | *Session management* | As required based on session management strategy (see decision framework) | | *Front-channel logout* | Very specific use cases | | *Back-channel logout* | As required based on session management strategy (see decision framework) |   **OAuth Authorisation Server**   |  |  | | --- | --- | | Core Grant Types | Applicability | | *Authorisation code* | Covers most common use cases and application clients | | *Implicit* | Covers most common use cases and application clients | | *Resource owner* | Advisable for trusted clients only to support username/password credential authentication (where the IdP acts as a credential provider). | | *Client credentials* | Advisable for unattended services and non-interactive clients (e.g. CLI’s, daemos or backend services) that need access to an API | | *Refresh token grant* | Advisable for mobile apps and SPA’s supporting persistent sessions (see decision framework session management strategy)  Required for IdP to IdP federation (see pattern library) and to maintain currency of attribute information  Required for RP to IdP federation to maintain currency of attribute information | | Extension Grant Types | **Applicability** | | *Token revocation:*  *RFC 7009 OAuth 2.0 Token Validation* | Strongly advisable and as required based on session management strategy (see decision framework) | | *Bearer token security:*  *RFC 7636 Proof Key for Code Exchange by OAuth Public Clients (PKCE)* | Strongly advisable for native mobile applications to protect against man-in-the-middle (MITM) attacks as OAuth codes and tokens pass through the operating system as part of the custom URI handling process. | | *Protocol translation:*  *RFC 7522 SAML 2.0 Bearer Assertion Profile*  *RFC 7523 JSON Web Token (JWT) Bearer Profile* | As required to support leveraging existing Web SSO sessions for API Authentication (see pattern library) | |
|  | Agencies are to manage lifecycle of staff and/or contractors in accordance with the QGAF Evidence of Identity (EOI) requirements (see Appendix E of QGAF).  All Agency Staff IdP(s) are required to be federated with QGSFAS and meet minimum requirements - agencies must provide:   1. A standards compliant Federation IdP for Web Single Sign-on (SAML or OIDC) which is capable of the following:  * SSO authentication for agency managed Microsoft windows via Windows Integration Authentication (WIA) * SSO authentication for agency managed mobility devices based upon X.509 certificates * RSO authentication for remote users from an internet or non-home agency network origin * Multi-factor authentication (where deemed required by the agency)  1. A RSO LDAPS interface (typically AD) to authenticate users via username/password credentials 2. A read-only LDAPS interface to a directory that is fully integrated with a corresponding identity lifecycle management system for attribute retrieval/query of:  * core biographic details (this information constitutes no more than the information currently published to GovNet) * Authorization information for role-based access control (RBAC) based upon Active Directory security group membership * video conferencing endpoints information to populate the phonebook  1. A public key infrastructure (PKI) Certificate Authority capable of:  * issuing device/machine certificates * providing GovNet or internet accessible Certificate Revocation services (CRL or OCSP protocols)  1. A collision-resistant, unique and persistent identifier for each identity (unique refers to the uniqueness of the identifier key itself, not the need to guarantee an individual has only one unique identity (although this should be the goal). This identifier shall be an RFC 822 compliant Email Address. This identifier must be:  * the primary identifier represented in federated authentication assertions (e.g. NameID for SAML) * the username field binding for the RSO interface * the lookup key for attribute queries * the owner of any print jobs (when using the ICT Buildings Follow-me print solution the user’s user principal name (UPN) in AD must be set to their email address due to Microsoft Windows print driver integration)   Note: Requirement 1 is not required for agencies electing to utilise the Hosted IdP option. Requirements for the Kerberos WIA option are outlined in the 1WS agency integration specification (AIS).  Agency managed devices (e.g. Microsoft Windows-based PC’s) to support  Wired & Wireless network access requires an:   * IEEE 802.1X supplicant configuration for EAP-TLS authentication * X.509 certificate (User or Device – unique per device) issued and signed by the Agency CA |
|  | The requirements and standards for Client Identity Management Systems varies depending upon the role:   |  |  | | --- | --- | | Role | Applicable standards | | *Relying party application for online services using a Customer Identity Provider* | * See Relying Party Application Resource standard. * An applicable pattern to link customer and client identifiers (see pattern library) | | *Attribute Provider to a Customer Identity Provider* | * An applicable pattern for authoritative source integration. * Attribute metadata should be provided | | *Relying party API 3rd party access via Customer Identity Provider authorisation* | See Relying Party API Resource standard | | *Attribute Provider to another Client Identity Management system* | As per the QGEA policy for Customer Details Management agencies must ensure that exchange of customer details between agencies occurs in standardised way by adopting the Queensland Government chosen Customer Data Model (Australian Standard Interchange of Client Information - AS4590:2006) as the basis for interfaces exchanging customer information. | | *Consumer of 3rd party Attribute Providers (authoritative sources)* | The 3rd party determines the interface requirements. | | *Attribute Provider to 3rd parties* | Due to diverse business requirements it is not possible to establish interface standards for 3rd party relying party access. | |
|  | As a consolidated whole-of-government service offering, the QGov Customer Identity Provider must support a wide range of agency business requirements, compared to Agency Customer Identity Providers which need only meet the requirements of a particular agency.  Due to the importance of the QGov service and dependency by multiple agencies, the following requirements are considered mandatory to maximize interoperability and ensure assurances of identity and credential can be shared:   * Multiple methods for interfacing (direct API, widgets, hosted pages) * Federated Authentication and Single Sign-on for Application Resources (which meet the outlined relying party standards) * API Authentication & Authorisation for API resources (which meet the outlined relying party standards) - support for the following patterns: * Single API access using QGov as the IdP (all patterns 1-5) * Multiple API access using QGov as the IdP (all patterns 1-3) * Access to a common API using QGov via another IdP (pattern 3 only applicable) * Access to an API using QGov and another IdP (all patterns 1-3) * Native mobile application support (1st party and 3rd party developed) with support for Proof Key for Code Exchange (PKCE) for security * Authorization/consent model for customer-controlled sharing across agencies (profile attributes and relying party APIs) * Credential Broker as per the blueprint * Identity Broker as per the blueprint * Support for relying parties which includes agencies, other jurisdictions and third parties. * Support for: * anonymous or pseudonymous access * authenticating individuals and businesses * online and in-person identity proofing |
|  | To ensure a consistent customer experience within the Queensland Government, Agency Customer Identity Provider federate with:   * the QGov Customer Identity Provider (bi-directional) where each IdP accepts the other's credentials and/or identities and; * any other Customer Identity Providers where there is benefit due to an overlapping user base or existing user population   Refer to the pattern library for a model to federate two Identity Providers (see Federated Authentication IdP to IdP for more information).  Agency Customer Identity Providers must meet the following minimum requirements:   |  |  | | --- | --- | | Requirement | Description | | *Offer Customer Choice of Credential (Credential Brokering)* | The IdP should accept/broker one or more 3rd party credentials (relevant for their user constituency) to provide the user a choice of credential and the ability to bring-their-own credential rather than needing to register a new credential specific to the IdP.  This may include brokering federated credentials of other Queensland Government Customer IdP’s appropriate for the user constituency. | | *Prove-yourself-as-required (Identity Brokering)* | The IdP EOI and user enrollment processes should allow an individual to re-use previous identity verifications through acceptance of one or more of the following methods as evidence:   1. paper credentials/documents (matched against source issuer) 2. digital identities (linked via a credential or matched against source issuer) | | *Web Single Sign-on* | 1. The IdP should provide single sign-on across relying party applications (where appropriate given the assurance level). 2. The IdP should support IdP-initiated SSO to relying party applications to allow another IdP to ‘smart link’ directly to the application with a pre-selected IdP rather than require the user to manually select the IdP if multiple IdP’s are brokered. 3. Session timeout alignment of 20 mins | | *Privacy-by-design* | The IdP should support the following privacy enhancing features:   1. anonymous or pseudonymous access where appropriate 2. user consent over sharing of attributes with external parties 3. use of derived attributes and assertions as required 4. unique pairwise identifier algorithms per RP to ensure RP's cannot use a shared identifier to cross-identify users without user consent. | |
|  | Requirements for Partner IdP’s will vary based upon the chosen integration option. When using federation provisioning, refer to the standards section regarding preferred federation protocols.  If the Partner IdP is integrated with QGov as a credential provider as per Pattern 3 for Agency Staff & Partners, please see the federation protocols supported by the QGov federation service in Appendix X. |

## Relying parties

Relying party resources requiring authentication should support claims-based authentication based upon industry standards to enable the ability to accept an asserted identity and credential from a trusted Identity Provider (the same organization or another entity).

Agencies should consider establishing:

* procurement standards for 3rd party applications
* development standards for 1st party applications.

| Element | Requirements |
| --- | --- |
| Application resources | Applications should support claims-based authentication to:   * improve user experience and productivity through SSO across different devices: * eliminating time spent re-entering user credentials and password fatigue from having to store or remember different usernames and passwords * reducing password fatigue from having to store or remember different usernames and passwords * Reduce complaints about password problems, password-reset and service desk calls * avoid the need for users to separately register for services * provide the ability to accept: * trusted identities from another party * accept different (or multiple) credentials from the same or another party * improve security through: * Providing the ability to adjust security adaptively based upon user, device, location, time of day * supporting automated access revocation and lifecycle management * assisting to guard against phishing and credential harvesting attempts * reducing the risk of stored or cached passwords in applications and devices   In particular, hosted 3rd Party Applications (e.g. Cloud Services) should support claims-based authentication to ensure government credentials are never known or stored repeatedly by external providers untrusted or shared environments. This is a pre-existing requirement as per the Queensland Government Cloud Computing Implementation Model. |
| API resources | API resources should support claims-based authentication (i.e. OAuth) rather than rely upon authentication via client supplied credentials to:   * avoid transporting and storing credentials * enable access to be delegated using a resource delegation protocol (where required) * enable access to be revoked or renewed as required * avoid propriety and possibly insecure non-standard token formats   API’s which facilitate/broker customer access to data should support a resource delegation protocol i.e. OAuth (or OIDC or UMA which are supersets) such that:   * the customer (the resource owner) can to authorize/delegate/consent to an intermediately such as a 3rd party application, individual, organization or agent to act on their behalf * the delegated access can be based upon a finite set of permissions, be time-based and/or revocable by the customer. * the customer has a choice of the party which is entrusted to manage delegation over their resources (where appropriate). This requires use of the UMA protocol based upon OAuth.   The OIDC protocol which is a superset of the OAuth protocol should be considered the default protocol choice for resource delegation where available. ODIC provides an improved token format which allows for the conveyance of rich attribute information such as identity information in addition to OAuth tokens which only covey resource permissions. Basic OAuth support is more pervasive.  The above guidance applies to REST-based API’s as SOAP-based API’s (authenticated using WS-Trust) are considered legacy. The Decision Framework still outlines mechanisms to support existing and 3rd party SOAP-based API’s via token translation and options for SOAP-based API’s to support modern OAuth protocols. |
| Whole-of-government or cross-agency applications | Any whole-of-government or cross-agency applications which need to authenticate or register Queensland Government Staff should utilize federated authentication to:   * Provide a similar single sign-on experience common to local agency resources * Avoid duplicate registration * Reduce password fatigue and duplicate passwords   These applications should use the QGSFAS service for authentication as per the pattern library, although direct peer-to-peer federations between agencies are supported. To be compatible the applications must meet the above standards for Application Resources. |
| ICT for Buildings Service Providers | Any ICT for Buildings Service Providers engaged under the ICT for Government Buildings SOA may utilise the full functionality of QGSFAS authentication service (interfaces for SSO, RSO, Attribute Query and Identity Orchestration). |
| Regional Connectivity Network Service Providers | Queensland Government appointed regional connectivity network service providers are responsible for operation of a Network Admission Control (NAC) system (RADIUS server) that authenticates wired and wireless devices and users to the network.  Admission onto an agencies nominated corporate network is to be based upon the certificate issuer and other nominated authorization policies.  Optionally the NAC can evaluate and remediate a device for policy compliance before permitting access to the network.  The provider must:   * supply local guest WiFi registration and account management * authenticate Corporate-Guest WiFi access by a Queensland Government employee using an unmanaged device via federated authentication using the QGSFAS (either via the Web SSO interface (preferred) or RSO LDAP interface) * authenticate managed devices to the Corporate Wired or Wireless network of the respective agency (data VLAN) based upon IEEE 802.1X using RADIUS and EAP-TLS authentication based upon X.509 digital certificates * maintain trusted certificate chains (the Public Key(s) for the respective agency Root and any sub Issuing CAs and Certificate Revocation services) for each agency. * verify machine certificates are valid (issued and signed by a trusted Queensland Government Agency CA), including revocation checking. * Provide MAC-address bypass rule management and traffic management security to authenticate utility devices (Print & Imaging Devices, AV Devices, VoIP phone handsets, PC for remote build) access to a common network, or a specific Agency network (voice or build VLAN) |
| ICT for shared Service Outlets | Queensland Government appointed ICT service providers (or lead agencies) for shared service outlets may utilise the QGSFAS service to support authentication requirements for the following ICT services:   * Wired & Wireless Network services (leveraging the supported integration used for Regional Connectivity Network Service Providers) * Print & Imaging Services (leveraging the supported integration used by ICT for Buildings Service Providers) * Shared applications (leveraging the supported integration for whole-of-government or cross-agency applications)   The provider of the above ICT services is independent to provider of the QGSFAS authentication service (which is currently supplied by a provider of ICT building services). |

## Federation schemes

| Element | Requirements |
| --- | --- |
| **Federation Schemes** | Identity Federation Schemes within the Queensland Government which broker communities of Identity Provides or Relying Parties should:   * natively support attribute metadata (providing metadata/translating different trust frameworks) or at a minimum; * route metadata by Identity Providers and Relying Parties adopting a dynamic trust model |
| **Federation Service (logical role)** | Identity or Credential Providers which perform the optional federation service role to broker Identity or Credential Providers within the Queensland Government are to meet the following minimum standards:   1. IdP discovery processes (interactive determination by the end user, and programmatic determination wherever possible) 2. support for IdP-initiated SSO (smart links) 3. identifier unlinkability across Relying Parities   Appendix X contains a list of well-known Federation Service Providers. |

## Identity federation protocols

This section covers standards and protocol considerations to improve interoperability. The industry has developed standards to address particular areas of complexity which become brittle and difficult to manage over time as. The majority of standards efforts have focused upon establishing and abstracting connections between IdP’s and RP’s to manage the growing number federation connections over time. As the scope of federation deployments increases, there will be pressure to further standardise overall federation practices to reduce operations overhead. Standards aim at consolidating requirements of suppliers, users, relying parties and government legislative bodies into frameworks that may be used for coordinated implementation of authentication schemes.

Agencies should continue to expect:

* To adopt de jure as well as de facto standards
* to be operating in a multiprotocol environment for the foreseeable future
* to see mainstream adoption of standards and implementations prior to being fully finalised or ratified
* multiple proposed and standards for unaddressed gaps e.g. federated OAuth/STS
* new extensions to existing standards such as OAuth and SCIM

As a general principle Queensland Government agencies should adopt industry standards where:

* they support desired use cases
* are widely supported by multiple vendors (mainstream adoption has typically occurred prior to formal ratification)
* the security and privacy requirements align
* they are interoperable.

The table bellows lists preferred standards for common use cases and alternatives or competing standards or implementations. Where there are multiple preferred or complete standards, refer to the decision framework for comparison information as to which standard bests suites particular use cases.

| Category | Preferred standard | Alternatives | Advice |
| --- | --- | --- | --- |
| **Authentication** | FIDO | None | FIDO is the first standards effort to standardise credential diversity/authentication schemes. Agencies building stand-alone digital credentials should consider compatibly. |
| **Provisioning** | SCIM | SPML (Legacy) | The use of JSON over REST for user management is a common direction. SCIM provisioning protocol uses this design pattern, but it has seen limited adoption. SPML (the previous standard) has seen low adoption for federation and directory |
| **Federated authentication** | OpenID Connect  SAML | OpenID Connect completes with SAML for Web SSO  WS-Federation (Legacy) | Open ID Connect and OAuth have emerged as the clear winners for providing authentication and authorisation for API-based applications. There are no competing protocols for OAuth and Connect; organisations can confidently develop applications using these protocols.  ODIC is preferred, however see decision framework as the most appropriate protocol per use case.  Note: The proposed NAPPS standard for mobile device SSO was officially dropped late 2015  Note: OAuth can be used to achieve federated authentication (typically for social media logins), although the standard is intended for API authorisation/resource delegation. |
| **Identity assertions** | JSON Identity Suite (JWT)  SAML Assertion | As above | Identity assertion token formats align to the federated authentication standard selected above. |
| **API authorisation** | OAuth/ OpenID Connect | WS-Trust (Legacy) | OpenID Connect supports a subset of OAuth flows (in some implementations, all OAuth flows are supported)  WS-Trust to protect SOAP-based Web Services considered legacy, given the explosion of REST-based API’s (and the corresponding uptake of OAuth). |
| **Delegated access and consent** | OAuth  UMA | None | See decision framework as to the most appropriate protocol per use case. |
| **Authorisation** | XACML/ JACML | ALFA | Wherever possible, use the modern JSON via REST profile of XACML 3.0 (referred to as JACML).  Note: ALFA - Axiomatics Language for Authorisation (ALFA) is a proprietary abbreviated language by vendor Axiomatics which is translated to standard XACML. |

1. Standard versions

The table below lists the versions of each standard and advice.

| Standard | Version | Released | Standards Body Status | Advice |
| --- | --- | --- | --- | --- |
| FIDO | 2.0 | 2015 | Draft, Ongoing Development | Use of v2.0 will quickly supersede v1.x due to adoption weight |
|  | 1.0 | 2014 | Active |  |
| SCIM | 2.0 | 2015 | Active |  |
|  | 1.1 | 2012 | Active |  |
|  | 1.0 | 2011 | Depreciated |  |
| OIDC | 1.0 | 2014 | Active |  |
| SAML | 2.0 | 2005 | Active, Stable |  |
|  | 1.0/1.1 | 2001 | Depreciated | Low use today. Majority is v2.0 |
| OAuth | 2.0 | 2012 | Active, Stable | Consider using ODIC 1.0 which includes most OAuth 2.0 and supports Federated Authentication. See DF. |
|  | 1.0/1.0a | 2007 | Depreciated | Known security vulnerabilities Low use today. Majority is v2.0 |
| UMA  (profile of OAuth 2.0) |  |  | Active, Ongoing Development |  |
| XACML | 3.0 | 2013 | Active | Use the latest version (3.0) |
|  | 2.0 | 2005 | Active |  |
|  | 1.0 | 2003 | Active |  |
| Shibboleth | V3 | 2015 | Active | Active in the higher education and/or research communities |
|  | V2 | 2011 | Depreciated. Support ends June 2016 |  |
| OpenID | 2.0 | 2007 | Depreciated | Migrate to OIDC (migration path from OpenID 2.0 to OIDC 1.0) |
|  | 1.0/1.1 | 2004 | Depreciated |  |
| WS-Fed | 1.x | 2007 | Depreciated | Vender centric (Microsoft) – low adoption. Migrate to SAML or OIDC |
| SPML | 1.0 | 2003 | Active, Low Adoption | Utilize SCIM |

For a complete inventory of relevant industry standards related to identity federation and related security domains, refer to the Identity Ecosystem Steering Group (IDESG) Standard Inventory: <https://wiki.idesg.org/wiki/index.php?title=Category%3AStandards>

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Key changes made |
| 0.0.1 | June 2016 | QGCIO | First draft |
| 0.1.0 | November 2016 | QGCIO | Draft for informal comment |
| 1.0.0 | May 2017 | QGCIO | No changes following informal or formal consultation. Administratively approved by Director, Strategy, Policy and Governance, QGCIO |