Queensland Government Enterprise Architecture

Federated identity blueprint

Information models

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 – Information models* 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 – Information models*

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](#_Toc484425207)

[1.1 Identity information 4](#_Toc484425208)

[1.2 Definition of identity 4](#_Toc484425209)

[1.3 Types of identity 5](#_Toc484425210)

[1.4 Entity relationship models 5](#_Toc484425211)

[1.5 Record identifiers 15](#_Toc484425212)

[1.6 Identity assertions 16](#_Toc484425213)

# Standards

## Identity information

Identity information is used to support several kinds of activities; the three most common are:

* Personalisation of user experience - requires that identities be persistent (so that the user gets the same, or better, experience over time), but it does not require that the identity be accurate. A Queensland Government Authentication Framework (QGAF) assessment can be used to determine requirements for contactabilty and service history.
* Authorisation - requires a higher degree of accuracy because enforcement of security policy and access depend on facts about attributes.
* Accountability (non-repudiation) – requires a high degree of accuracy such that there is undeniable proof the transaction/registration has occurred. Audit logs will be required to capture sufficient evidence to prevent the client from repudiating the registration and support any corrective and punitive actions. A QGAF assessment can be used to determine the risk of non-repudiation.

## Definition of identity

A digital identity is primarily a set of attributes that uniquely describe an entity (e.g. individual/organisation) within a given context.

An attribute is a characteristic or property of an entity, or data that can be associated with an entity e.g. name, date of birth, place of birth, home address, client number.

Identity attributes have varying characteristics, for example they may:

* differ depending on the type of real world entity being identified
* change over time (e.g. a postal address, role) or remain static (e.g. date of birth)
* be self-asserted, self-selected or issued by an authority
* be transient or permanent
* be suitable for human interpretation or only by computers.

Attributes do not have to be unique; it is common for different identities to share attributes, even for such important attributes as name or date of birth[[1]](#endnote-1).

A unique attribute is an attribute that has a one-to-one relationship with the identities in a given context (or domain)[[2]](#endnote-2).

Departments have to consider the risk associated with attributes — collecting and storing them, managing them, and making decisions based upon them.

### The properties of identity

Due to the subjective interpretation of a digital identity, the OEDC in 2007 published the following distinguishing properties of an identity.

An identity behaves according to a number of observable properties[[3]](#endnote-3), as follows:

* Identity is social. Humans are naturally social. To engage in social interactions (including commerce) people need something that persists and that can be used as a basis for recognition of others – an ‘identity’.
* Identity is subjective. Different people have different experiences with the same individual and therefore attribute different characteristics to that individual; that is, they will construct different identities for him.
* Identity is valuable. By building a history of a person’s past actions, exchange of identity information creates social capital and enables transactions that wouldn’t be possible without identity. In other words, identity lends predictability to afford a comfortable level of confidence for people making decisions.
* Identity is referential. An identity is not a person; it is only a reference to a person. Even if a person develops spin-off personas so that other people know him through those various digital identities, and even if others create profiles of a person, ultimately the collection of characteristics that signal who a person is need to point back to that person.
* Identity is composite. Some information about a person arises from the person himself; he volunteers it. But other information about him is developed by others without his involvement.
* Identity is consequential. Because identity tells of a person’s past actions, the decision to exchange identity information carries consequences: Disclosure of identity information in a certain context can cause harm; failure to disclose identity information in another context can create risk.
* Identity is dynamic. Identity information is always changing; any particular identity dossier might be inaccurate at any given moment.
* Identity is contextual. People have different identities that they may wish to keep entirely separate. Information can be harmful in the wrong context, or it can simply be irrelevant. Keeping identities separate allows a person to have more autonomy.
* Identity is equivocal. The process of identification is inherently error-prone.

## Types of identity

There are four common types of identities:

* persons (individuals) – employees, contractors, clients, customers, individual partners
* organisations – commercial or non-commercial organisations
* devices – smartphones, personal computers
* resources – applications, systems, documents.

## Entity relationship models

The following four diagrams depict the relationships and relevant entities for each of the core identity types (persons, organisations, devices and resource) from a primary viewpoint.

Common across all five models are these core entity types:

* digital identities
* digital credentials
* digital entitlements
* digital delegations.

### Person entity relationship model

A person entity may typically represent an employee, contractor, customer, individual partner (e.g. volunteer).

The terminology varies depending on context.

In context to customer identity:

* a resource will typically represent a service or product
* entitlements will typically represent links to products and services with an assigned role e.g. parent, child, vehicle or property owner
* links to other identities or organisation will typically represent delegated authority/relationships to authorise an intermediately to act on their behalf.

In context to employee identity:

* a resource will typically represent a line of business application
* entitlements will typically represent permissions to access applications and perform functions such as approve a timesheet
* links to other identities will typically represent reflect delegated authority to act on their behalf such as HR or Financial delegations while the delegate is on leave.



It is important to note the diagram reflects a single logical entity and relationship model, not a physical data model. The logical entities and individual attributes can be partitioned across multiple separate systems, and/or managed by different IAM processes. For example:

* The RP may also hold a local managed copy of the identity (shadow copy). The local identity may in turn:

store additional attributes relevant to the RP

have one or more local credentials provided by the RP e.g. local MFA.

* Entitlements for identities and the resources may:

be managed solely by the IdP or the RP or most commonly a combination of both

be modelled differently in either systems e.g. the IdP may utilise a coarse-grained authorisation model, whereas the RP may use a fine-grained model.

|  |  |
| --- | --- |
| Item | Description |
| **Identity** | *For customer identity:*  A person may construct multiple identities as they choose to carefully reveal or conceal personal information based on what they deem appropriate or minimum for a specific interaction and context to maintain privacy.  This identity is commonly referred to as a partial identity, persona, contextual or episodic identity. Each partial identity might have its own name, own identifier and own means of authentication.  Some use cases need to be able to differentiate members of the current population of users, but don't need to care whether a user has multiple identities at different times or even at the same time[[4]](#endnote-4). Systems in which identity is persistent and unique (e.g. tax systems which need to be able to track individuals over a lifetime) are more expensive than systems that allow users to create new accounts without tying them back to pre-existing accounts and histories; persistent identity should be implemented only when it's required[[5]](#endnote-5).  *For employee/contractor identity:*  A person’s identity is established by the associated organisation – typically through HR processes. A person may have multiple active or inactive identities across organisations, or agencies/sub-agencies. |
| **Credentials** | A credential is authoritative evidence of an individuals claimed identity. Credentials come in many types, from physical papers and cards (such as a passport or ATM card) to electronic items (such as a password or digital certificate), and often incorporate anti-tamper features[[6]](#endnote-6). |
| **Verification** | Identities have verification (confidence level) across one or more identity attributes based upon one or more attestations. Metadata to support verification may be stored. When using a dynamic trust framework model, this metadata may also be shared with a Relying Party. For more information, see Dynamic Trust Framework Model (Attribute Driven) |
| **Entitlements** | Entitlements   * An Entitlement (or privilege) represents the authorised behaviour of a subject. * Identities are assigned one or more entitlements (or can be interfered from the subject’s attributes). An entitlement may: * relate to a single resource e.g. an entitlement of purchase order release in SAP * apply to several resources e.g. an entitlement of ‘customer service’ may authorise service functions across multiple systems * represent a role e.g. payroll manger * represent a relationship e.g. parent, student, vehicle or property owner. * Access to resources require one or more entitlements determined by the resource access control policy.   **Modelling entitlements**  Entitlements can be modelled using either:   * **Identity Based Access Control (IBAC)** – where entitlements are assigned and managed on an individual basis * **Role Based Access Control (RBAC)** – where logically related collections of entitlements are grouped into roles and assigned to one or more subjects. Roles can also associate people of a certain job responsibility with a set of entitlements to a job function. A role itself can represent an entitlement. * **Attribute Based Access Control (ABAC)** – where a subject is granted entitlements at run time based on its attributes and other contextual information (e.g. the resource, devices, environment etc.) according to a security policy written in business terms which can be rapidly changed.   **Managing entitlements**  A subject’s entitlements are managed using a blend of both administrative and runtime authorisation capabilities.   |  |  | | --- | --- | | Administrative  Authorisation  (Static  Authorisation/Early Binding) | Authorisation decisions that are based on upfront information about the subject and the application.  For example, John works on the sales team as a sales person and has access the sales system | | Runtime Authorisation  (Dynamic Authorisation/Late Binding) | Reflects authorisation late-binding decisions based on information that is not available until time of access.  For example, John is in an airport trying to access the sales system from his personal tablet on the last day of the quarter after close of business |   Both Administrative Authorisation and Runtime Authorisation models are required. For example:   |  |  |  | | --- | --- | --- | |  | Administrative  Authorisation | Runtime Authorisation | | **Role Based Access Control (RBAC)** | Roles assignments  Policies which govern role assignments | Grant/deny access based upon group/role memberships | | **Attribute Based Access Control (ABAC)** | Write standard access policies  Government attribute data quality | Grant/deny access based upon a decision incorporating the subject, resource and context attributes | |
| **Link to self** | * In some cases, due to legislation or risk management considerations agencies may be required to identify a user as a previously known user (reassociation) such that records over a long period of time are to be traceable to one individual regardless of how many different accounts, credentials the induvial may have had overtime. * Reassociating identities to previously known identities may cause the possibility of error, cost of historical data storage, protection of historical data, development/maintenance of re-association procedures, and other measures that increase cost and complexity[[7]](#endnote-7). |
| **State (Lifecycle)** | * Identity information needs to be managed according to its lifecycle events defined by the ISO 29003:2012 standard: * Birth * Pre-education * Education * Employment * Marriage * Retirement * Death * Post death.   The expiry of identities requires careful consideration. The length of time that an identity should remain valid is dependent on a range of business requirements, must consider both the expiry of identities and of authentication credentials. Identities which are expired will be required to undergo a reactivation process should they need to be restored. Authentication credentials which are expired will also need to be reissued.  For many use cases, an identity never expires, but only the associated authentication credentials are expired. This commonly occurs with passwords, with many organisations requiring passwords to be reset on a regular basis (for example every 60 days). It is however possible to expire the identity itself, which will in turn automatically prevent the use of any authentication credential in use. This may be the most practical approach when authentication credentials in use do not have an easy means of expiry (a biometric for example).  Where identities are not given an indefinite active life, there are two common approaches to expiry:   1. An identity has a set life based on the date of registration. Typically, expiry in these circumstances is set in years. 2. An identity’s active life is refreshed by use of the identity, but expires after a certain period on non-use. Typically, expiry in these circumstances is set in much shorter periods such as days or weeks. An example may be where a client has not ‘logged-in’ to a service for 12 weeks, the identity is automatically deactivated, and a re-registration or re-activation process must be conducted to re-activate the identity. Likewise, similar approaches can be taken to the expiry of authentication credentials.   See Section 4 QGAF: Identity and Registration Concepts for more information of deactivation and reactivation processes. |
| **Subject Attributes** | Attributes associated with a person may include attributes across the following categories. Attributes can also assist with access control decisions where access policy requires knowing specific things about subjects from other domains.  **Identity attributes**  Attributes of a person related to identify/authenticate a person:   * Biographic information such as Name (First, Middle, Last) and Date of Birth * Biometric information such as a Photograph and signature   *Example for an employee*   * ID number * Gender * Postal or Residential Address * Job Position * Department * Work Location * Work phone number * Personal/work mobile number * Work email address * Tax File Number   *Example for a citizen*   * Date of Birth * Place of birth (city, country) * Citizenship/Immigration status * Gender * Email address * Residential/postal address * Current/Previous address * History of names * Race * Dialect * Nationality * Date of Birth * Country of Birth   These represent intrinsic attributes about people such as department, organisational unit and job code and are not necessarily assigned administrative or runtime authorisation entitlement mechanisms, but may be used for assess control decisions. Intrinsic attributes by their nature cannot be revoked easily.  Phone number and e-mail address are not used as part of the identity proofing process, but as part of credential management (issuance process).  SCIM standard provides an optional standard user schema that should be used as a starting point for schema design.  **Authority attributes**  These attributes represent explicit entitlements which are assigned to or revoked from subjects through administrative or runtime authorisation entitlement mechanisms.  *Proof of Role (representing relationships):*   * Parent/legal guardian * Business Director * Parent * Student * Vehicle Owner * Property Owner * Organisational Position/Level * Approval Limit * Project Manager/Project sponsor   *Proof of certification (assignment, and qualifications):*   * Proof of professional license * Proof of training certification * Proof of profession body registration   **Preference attributes**   * Attributes related to a user preference which are often self-asserted for service personalisation such as: * Preferred name * Preferred services * Preferred contract channel * Attribute release preferences (e.g. ask me every time, only the first time)   Preference attributes may not be stored in an IAM system, but rather a CRM or profile management system. |
| **Context Attributes** | Authorisation requirements often need to take into account not only personal and resource attributes, but also operational or situational contextual information such as:   * Time of day * Geolocation of the subject (Country or a particular Workplace building) * Transaction value/risk score * Connection security of the subject (Connecting using VPN) * Authenticator type * Operational Status e.g. Declared Disaster Event, Threat Level 1 |

### Organisation entity relationship model

An organisation entity may typically represent a business interacting with government or a partner organisation or another government organisation. The delegation model is more applicable to businesses interacting with government.



|  |  |
| --- | --- |
| **Responsible Officer** | An organisation has one or more responsible officers which can act on behalf of the organisation in their appointed capacity such as the business owner or company director or secretary.  The same individual may also hold similar officer roles for other organisations, for example where the individual operates multiple businesses. |
| **Delegated Organisation** | An organisation could also act on behalf of one or more organisations, for example:   * a tax agency/agents * a parent organisation with multiple individual sibling organisations.   For accountability reasons this relationship may be reflected at an individual level through an authorisation model such that specific individuals have delegation. |
| **Entity Type** | An organisation entity for taxation purposes will have type of entity or business structure. The primary categories of entity are listed below[[8]](#endnote-8). There are many sub-types for each category.   * non-profit organisations * individual (Sole trader) * company * trust * partnership * superannuation entity * deceased estate. |
| **Attributes** | Attribute will vary based upon the Entity Type.  For an example information model and schemas consider the:   * Australian Business Register (ABR) * Australian Charities and Not-for-profits Commission (ACNC).   *Example attributes:*   * name (trading, entity legal name) * address and geocoding * taxation status * ABN, ACN, ARBN * web address * telephone numbers * buildings and offices * business activity * financial activity * organisation members * organisation history * Australian and New Zealand Standard Industrial Classification (ANZSIC) code and description. |
| **State (Lifecycle)** | Identity information needs to be managed according to its lifecycle events defined by the ISO 29003:2012 standard:  An organisation has the following states:   * creation * operation * administration * dissolved. |

### Resource entity relationship model



|  |  |
| --- | --- |
| **Attributes** | Examples attributes associated with a resource may include:   * identifier * information security classification * geographic location * a class of application or resource * a document resources may have these attributes: * document owner * assigned editor * status (draft) * rights to copy/modify.   A purchase order resource may have these attributes:   * PO amount * PO location * PO creator * PO status * PO ID. |
| **Access policy** | Rules or relationships that determine whether a requested access should be granted. |
| **State** | Identity information needs to be managed according to its lifecycle events defined by the ISO 29003:2012 standard:  A resource has the following states:   * creation * operation * revocation. |

### Device entity relationship model



|  |  |
| --- | --- |
| Item | Description |
| **Device attributes** | It is becoming more common for authentication and authorisation decisions to take into account the identification of the subject’s device. Device attributes can provide important context about user access such as:   * the organisations identifier and fingerprint * type (managed for unmanaged) * compliance status to policy * healthy security posture.   Device attributes may be supplied by mobile device management (MDM) software that supports device identification is needed. Some federation software vendors also support a level of device registration. |
| **State** | Identity information needs to be managed according to its lifecycle events defined by the ISO 29003:2012 standard:  A device has the following states:   * creation * operation * revocation. |
| **Local subject identities and credentials** | A device can be seen as a resource itself requiring authentication and often accepting local credentials against a registered identity. |

## Record identifiers

An **identifier** is a unique attribute that can be used to locate a specific identity within its context FICAM.

The following aspects need to be considered:

* assigning identifiers
* maintenance of identifiers
* collection, use and disclosure of identifiers (and other identifying information)
* validation of identifiers.

### Identifier types

Some services require the user identity; others can be accessed anonymously or pseudonymously but can also be used in an identified mode. The three common types of identifiers[[9]](#endnote-9):

* **Personal identifiers** - A personal identifier does not obscure the real-world identity of the person, resource or device. For an individual, it contains PII, such as a person's name, Tax File Number etc.
* **Pseudonymous identifiers** - A pseudonymous identifier provides a persistent identifier that obscures the real-world identity of the person, resource or device for privacy or security reasons.

There are many use cases where it is important to know that a returning user is an actual person that has visited before, but it is not important to know which particular person is represented by the user.

* **Anonymous (unidentified) access** - An identity assertion that contains no identifier of its subject obscures the real-world identity of the person, resource or device for privacy or security reasons.

For privacy purposes, the anonymous assertion is stronger than the pseudonymous one, whereas the assertion containing a pseudonymous or personal identifier is stronger for accountability purposes[[10]](#endnote-10).

### Uniqueness

Identifiers have a scope - Identifiers can be considered either:

* **Universally unique shared identifier (UUSID)** - guaranteed to be unique across all domains (including outside Queensland Government). For example, an email address and business domain names.
* **Locally unique shared identifier (LUSID)** - only guaranteed to be unique within a local domain which issued and manages the identifier. For example, Department of Transport Customer Reference Number (CRN) within the Transport Registration and Integrated Licensing System (TRAILS).

### Selecting identifiers

The following are principles to be considered when selecting identifiers:

* Identifiers have a scope - not every identifier is globally unique. Local identifiers are common used for privacy to prevent inadvertently linking and aggregating identity information across data contexts without user consent.
* Identifiers can co-exist – it may be necessary to map (or maintain a link) between identifiers in different domains. One common federation scenario is the need to map an identifier (LUSID or UUSID) for a subject known/asserted by an IdP to the local identifier (LUSID) the RP party uses to identify the subject – particularly when the subject’s identity has previously been already registered at the RP or the RP’s identifier is well established and known to identify records or there are technical constraints/storage formats to replace RP LUSID with the IdP’s LUSID or UUSID. For example, mapping the UUSID used by the QGCIDM IdP named the Queensland identifier (QID) to a TMR CRN. This process is undertaken by a RP is known as identity enrolment. For more information, refer establishing a link - identity enrolment at the RP.
* Identifiers may be private – various identifiers, although well-established within one domain may be considered private and selectively shared with other domains e.g. an individual’s Tax File Number or Medicare Number
* Not every identifier has to be human readable – It common in federated models for identity providers to use pseudonymous identifiers generated using pairwise algorithms for subjects to provide a double-blind scenario.

### Established identifiers

Appendix A contains a list of well-known and established identifiers for person and organisation entities. Wherever suitable, established identifiers should be used appropriately or mapped between domains where required. Re-use of common subject identifiers is important to avoid re-enrolment and improve support for standalone attribute providers.

## Identity assertions

Assertions securely carry and assert identity information across domains - typically between the identity provider and relying party to communicate a successful authentication event and represent the identity to a RP. An assertion contains a set of claims (or statements) about an authenticated subscriber. Claims are represented as simple key/value attributes.

Identity assertions are used to support federated authentication use cases and delegated authorisation use cases where the delegate or requesting party needs to be authenticated.

An assertion primarily contains one or all three types of claims:

1. Authentication claims - includes information about the successfully authenticated subscriber and authentication event (authentication method/means and time etc).

For example, the subject ‘John’ was authenticated using a password at 10:32pm on 1/4/2016.

The assertion contains an identifier representing the authenticated subject – see [Assertion Identifiers](#_Identity_assertions). The assertion typically also contains additional information related to the issuer (the IdP), audience the assertion is indicated for (the RP), validity and expiration periods.

Identity claims - contains specific additional characteristics related to the subscriber.

For example, subject ‘John’ is associated with these attributes:

First Name = John  
Middle Name = Gray  
Last Name = Smith  
DOB = 12/3/1976

1. Identity Attributes

For assertions representing a person, these attributes represent verified information from the IdP to identify the authenticated subject (typically biographic information).

#### Preference attributes

The assertion may also include preference attributes - attributes related to user preferences which are often self-asserted and used for service personalisation.

See [Standards](#_Standards) for an example attribute profile for Identity claims.

Identity attributes also be used for provisioning to establish a local identity in the RP’s resource or resource domain. See [Is Provisioning Required](#_Determine_Identity_Provisioning).

As these attributes will typically reflect PII, it is suggested:

RP should be requested only the minimum attributes required (mandatory or optional) – see decision framework for [Protocol Selection](#_Determine_Protocol) (which support this)

The user should be informed about the transfer of information to the RP, and, if required, consent be obtained on the basis of mandatory or optional information.

Identity claims may not be present for pseudonymous or anonymous access; or where Identity Proofing is conducted at the RP as opposed to the IdP.

1. Authorisation (entitlement) claims - identify specific resources the subscriber has permission to access at the RP. These resources may include specific applications, functions, documents or files. This information along with the identity claims is used as input into the RP’s access control decision which also augments other attributes associated with the resource itself and the contextual environment.

For example, a verified claim that the user is in fact a currently licensed medical doctor, which would be required to completing a medical research workflow task that can only be performed by a medical doctor.

During the RP’s authorisation processes these authorisation claims from the IdP are transformed into a local authorisation model which is understood by the protected resource (or resource domain). For example, subject ‘John’ has these authorisations:

Claim Local Authorisation Model   
(Issuer = Organisation A) 🡪 (Cost Centre = 123456)   
(Group = Sales Team) 🡪 (Roles = Place Order, Track Order)   
  
The local authorisation model is specific to a given application, which generally aligns to either identity-based, role-based or attribute-based access control.

Provisioning actions may be required to assign an entitlement to local identity (e.g. assign a role) in the case of identity-based or role-based access control models.

In some cases, an identity assertion may only contain the information required to authenticate the subscriber (the authentication claim). In this case, the identity and authorisation claim attributes (or a subset) are fetched at a later time by the RP when required using an access token provided institute.

An assertion can also include access tokens for other delegated resources requested by the RP at time of the authentication event. For example, access tokens to authenticate the user to other API’s.

All identity information contained within an assertion must be protected and securely exchanged in a confidential and tamper evident manner, and protected from unauthorised access

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 |

1. https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2415-queensland-government-authentication-framework [↑](#endnote-ref-1)
2. https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2415-queensland-government-authentication-framework [↑](#endnote-ref-2)
3. The Properties of Identity were articulated by Bob Blakley, Jeff Broberg, Anthony Nadalin, Dale Olds, Mary Ruddy, Mary Rundle, and Paul Trevithick. Content is licensed under a Creative Commons Attribution 3.0 License. [↑](#endnote-ref-3)
4. <http://www.gartner.com/document/2076131?ref=solrAll&refval=169116108&qid=959e2abfb90ad1828ee9a5ee8bf4d0b1> [↑](#endnote-ref-4)
5. <http://www.gartner.com/document/2076131?ref=solrAll&refval=169116108&qid=959e2abfb90ad1828ee9a5ee8bf4d0b1> [↑](#endnote-ref-5)
6. https://gsa.github.io/ficam-arch/services/credentials/ [↑](#endnote-ref-6)
7. http://www.gartner.com/document/2076131?ref=solrResearch&refval=174822516&qid=a52f3edf679374e9ccf4122a4c87c514 [↑](#endnote-ref-7)
8. https://abr.gov.au/For-Business,-Super-funds---Charities/Applying-for-an-ABN/Business-structures/ [↑](#endnote-ref-8)
9. http://www.gartner.com/document/3029229?ref=solrAll&refval=174827356&qid=19eb5890eaa3ce6d8cd5747311abca20 [↑](#endnote-ref-9)
10. http://www.gartner.com/document/3029229?ref=solrAll&refval=174827356&qid=19eb5890eaa3ce6d8cd5747311abca20 [↑](#endnote-ref-10)