Document:

Reference Architecture

Part:

Identity Reference Architecture

Dated:

April 2022

Company contact:

Chief Technology Officer

cto@downerdefence.com.au

Contents

**No table of contents entries found.**

Figures

**No table of figures entries found.**

Tables

**No table of figures entries found.**

# Identity Reference Architecture

References:

## Introduction

As more activities are digitised there is a greater need to have digital identities so Enterprise can protect its data and information. Many of our enterprise’s current systems already use of accounts as a form of digital identity to assert authority and access rights; however, there is limited consistency across systems which requires users to maintain multiple accounts creates confusion and increases complexity. The need to have a trusted concept of a digital identity will be critical for all electronic transactions, across all battlefield systems. This will be especially as the ability to conduct cyber warfare increases. The trust of the digital identity and the processes governing it will need to be high, as it will form the basis of defence against cyber warfare and general internet-based attacks.

1. People can assert any identity; but they are who they are regardless of how they represent themselves. People may also have multiple and concurrent functional relationships with Defence. A person’s functional relationship with Defence will be defined as Persona. While this document is the Identity Reference Architecture, to clearly disambiguate the concepts, Persona will also be discussed.
2. This reference architecture will introduce the Identity and Persona concepts, their distinct characteristics and uses. It will introduce the taxonomy associated with them for use in solution designs, policies, and other reference architectures.

### Definition

Identity represents the uniqueness of an entity’s existence. Typically, there is a set of distinguishing identifiers (or attributes) that make identity determination and discrimination possible. However, even in the case where no identifiers are evident, separate entities still have separate identities. For example, identical twins represent two identities even though distinguishing identifiers are not always readily evident.

### Scope

This paper is only concerned with Identity of Defence Entities. This is part of an overall discussion on Identity and Access Management (IAM). However, Authorisation (Access Management) and Authentication (another related topic) will be covered in separate Reference Architectures.

### Audience

Business and solution architects and requirements writers and solution providers should all be aware of the content of the Reference Architecture.

## Concepts and terminology

To facilitate consistent usage across our business and reduce issues arising from misunderstandings in how Identity applies to the enterprise, an agreed taxonomy is required. The application of taxonomy to solutions and other reference architectures will enable the consistent application of appropriate guidelines, patterns, and standards to future solutions, simplifying the integration of systems across our business.

1. *Entities* interact with Defence. *Identity* is about **who** those entities are; *Persona* is **what** their relationship is with our business. *Digital Identity* is the electronic representation of an Entity’s Identity, and which may only be assured to a certain level. All of these can form part of any access decision across the enterprise.
2. This Reference Architecture will introduce:
3. Entities,
4. Identity,
5. Persona,
6. Digital Identity, and
7. Identity Assurance.

## Reference Models

This taxonomy will form the reference model for Identities and their related concepts.

### Entities

In an ICT solution there can be many types of actors that utilise the business functions of the solution, however, there are only a finite set of actors that need identities. Generically, these actors are known as *Entities* and are further categorised as:

1. **Person Entity.** A human being for whom Defence establishes a Digital Identity.
2. **Non-person Entity.** Any non-human entity for whom Defence establishes a Digital Identity. Typically, this would be an entity that needs to assert authority, gain access, or have activities audited. Within the enterprise it will more often be executing system software that needs an identity – an ***Agent***.
3. Various references define large sets of non-person entities, but typically these references are referring to are just a passive object. When they do need to assert an identity, then it will be a software agent acting as the entity.

### Identity

As discussed, Identity is the basic understanding of who the entity is. Establishing identity is important as it may be used for:

1. **Asserting authority.** This is about establishing the legitimacy of the Entity deciding or issuing a command and therefore their authority to do so. Although a persona may represent the role and authority that the identity is undertaking, it is necessary that the persona is linked to the identity to establish the actual entity exercising the authority.
2. **Access control.** Access controls are the controls and surrounding processes that provide or deny entities the capability or opportunity to access or interact with resources. Establishing identity is often a major requirement for access control. Rules that define and enforce access control may also rely on other attributes associated with the entity. For example, a person’s clearance level may be used to determine trust.
3. **Auditing.** Being able to review activities for many purposes (e.g., performance, security, and legal analysis), requires an unambiguous and trusted ability to identify the entity involved.
4. Reference C defines some of the potential consequences of incorrectly establishing an identity:
5. **Fraud risks.** An entity without entitlement receiving a financial payment or other non-financial benefit because of a transaction (e.g., payment of a benefit or grant).
6. **Security risk.** An entity gaining unauthorised access to information, facilities, goods, or services, particularly of a sensitive nature.
7. **Privacy risk.** An entity gaining unauthorised access to confidential information of another entity.
8. **Downstream risks.** An entity using an identity credential or record issued or created by one organisation to commit identity crime against another organisation.

### Persona

Different entities can at various times have a different functional relationship with Defence. Typically, these would be at separate times – A military member retires and works in Defence as an Australian Public Service employee for a period. Subsequently, this person undertakes a contracting role. In this situation the one Person Entity with single Identity has multiple *personas* over time, but only one persona is *active* at any one time no matter how short that time may be.

1. In our business there are examples where identities can have multiple active personas.
2. *insert example*
3. additionally, a visitor persona could apply at any time as well.
4. The primary non-person identity that is relevant in our business is an agent. Agents are functionally specific; they do not change career or maintain multiple active relationships with our business. Therefore, agents cannot maintain multiple personas within our business.
5. As personas represent a functional relationship with our business, they are a business level concept and do not constitute separate identities of the Entity.

### Digital Identity

An Entity’s *Digital Identity* is the electronic representation of the Identity within the enterprise’s ICT Environment. There is to be only one Digital Identity per Entity. Therefore, an Entity’s Identity needs to have enough verified identifiers (credentials) so that when an Entity re-engages with Defence it is possible to reassociate the Entity’s Identity with its Digital Identity. These identifiers may vary with Entity type.

1. Once a Digital Identity is established for an Entity, it is to form the primary identifier for all authority assertions, resource access determinations and auditing. This will be achieved through provisioning systems that will use the Digital Identity as the primary identifier when provisioning accounts and access rights.

### Identity Assurance

As people have no natural globally unique identifier from birth[[1]](#footnote-2) (That technology can readily establish yet), correctly establishing their Identity to create or reassociate them with a Digital Identity will sometimes fail (whether fraudulent or accidental). The likelihood of failure proportional to the level of confidence in an Entity’s Identity is known as the *Identity Assurance Level*.

1. The nature of the physical credentials offered by the Entity and the level of verification to which they are subjected, results in different Identity Assurance Levels. These levels taken from Reference C are detailed in Table 1.
2. Table 1: Defence Identity Assurance Levels

| **Assurance**  **Level** | **Controls** | **Party** | **Note** |
| --- | --- | --- | --- |
| **Low** | Self-claimed or self-asserted identity | Public | Digital Identities will **not** be established for this level of assurance |
| **Medium** | Evidence of identity through use of identity information or documents from authoritative sources | our business | Digital Identities will be established; however, they will not support re-association. |
| **High** | Evidence of identity through use of identity information or documents from authoritative sources + information or documents verified with an authoritative source | our business | A **biometric credential is to be collected** to ensure future re-association of an Entity with their Digital Identity is successful |
| **Very High** | Evidence of identity through use of identity information or documents from authoritative sources + information or documents verified with an authoritative source + individual witnessed in-person | our business |  |

1. The detailed process of establishing these levels of assurance is outside the scope of this document. See Reference C for further details.
2. **Parties.** In relation to Parties as defined in Reference A, the following applies:
3. **Defence Party.** An Entity that our business has issued an Identity (meaning Digital Identity). Establishing a Digital Identity requires a Medium or higher level of assurance.
4. **Partner Party.** our business does not issue Digital Identities for Partners; however, when establishing a federated relationship with partners, their identity assurance levels must be mapped to Our Identity Assurance Levels. This enables risk-based assessments for federated access control.
5. **Public Party.** No formal Digital Identity within our business.

### The model

The following stylised UML class diagram captures the relationships between the taxonomy elements defined so far.

1. 

Figure 1: Identity Model

1. The following example illustrates the use of the major elements. A Fictitious Boot Management System (FBMS) initially operates as follows:
2. Military members have their boot sizes recorded in the FBMS; hence these Person Entities are subjects in the system. However, a few of the military members (persona) and some contractors (persona) Person Entities have access to the system to operate it and are therefore actors in the system. The actors have an account derived from their Digital Identities, the subject does not (this is a design choice and not a requirement).
3. FBMS is upgraded so military members can use the system directly to update their boot size and request new boots. As a result, they are no longer just subjects in the system but actors and now also have an account derived from their Digital Identity.
4. One of the contractors is a reservist; therefore, can request and approve the issuing of boots. As the one person can now request and approve the issuing of boots there is a separation of duties concern. As the two active personas represent the same Entity and therefore have the same Digital Identity, governance processes can identify and deal with the issue.

## Digital Identity Management

Digital Identities need to be established for Entities at their first substantial engagement with Defence. What constitutes a substantial engagement will be different for each person and is a business process decision for the business area managing the persona type. The activities undertaken leading up to the establishment (or re-association) of a Digital Identity will be known as *on-boarding*. Multiple on-boarding systems will exist.

1. It is likely that different on-boarding systems will form the definition of the persona for the Entity. For example, an entity on-boarded via a visitor management system will have a visitor persona, and entities on-boarded with an ICT orchestration tool are likely to be agents. It is expected that a single on-boarding system is responsible for one or more personas and that typically the same system is the ongoing management system for the Entities of that persona type. It is also expected that the opposite is not true, in that a single persona type would not be on-boarded by multiple systems (this is not a rule; however, it simplifies business processes and makes consistency of information management for the different personas more readily achievable).
2. Once on-boarded, the on-boarding system is not responsible for the management of the Digital Identity. The Digital Identity’s lifecycle will be managed independently of the on‑boarding system by the Identity Management System (IMS); however, the on-boarding system retains responsibility for its own business data for the Entity.
3. The on-boarding system is to maintain a reference to the Digital Identity so that the association is maintained. This provides the on-boarding system with an external reference to allow it to recognise duplicate Entities. The use of a central Digital Identity Key provides a common correlation identifier for auditing Entity activities. This will be the only mechanism Defence will have to develop a complete picture of an Entity’s activities across the enterprise.
4. Figure 2 shows an abstraction of the establishment of a Digital Identity. An on‑boarding system gathers the required information for the Entity and passes to the IMS, which verifies the documented information to establish (or reassociate) the Digital Identity for the Entity.
5. 

Figure 2: Identity Establishment

1. Once the Digital Identity is established the responsibility of the management of its lifecycle remains with the IMS.

### Digital Identity Lifecycle

The following lifecycle activities apply to Digital Identities:

1. are *created* at the first on-boarding and a level of assurance is established
2. can have their assurance level *upgraded*, but never downgraded
3. are *deleted* at death (person) or decommissioning (non-person).
4. Digital Identities are not records, activities pertaining to them are. The records do not need to be kept beyond Digital Identity deletion as they have no further business value.
5. Business systems leveraging a Digital Identity are responsible for their own records.

### Digital Identity Attributes

For the purposes of establishing and, when required, re-associating an Entity’s Identity with their Digital Identity, the IMS needs to capture foundation identity attributes. In Australia there are two primary sources of foundation attributes for Person Entities:

1. Birth certificates, and
2. Immigration documents.
3. From these documents, the intention would be to capture:
4. Name,
5. Date of Birth, and
6. Place of Birth.
7. As these attributes are created at a point in time, they are immutable. They are used to form a natural key that has a high likelihood (but no guarantee) of being unique.
8. For Agents, the equivalent to a Microsoft Windows Machine account would be used as the Digital Identity, so an appropriate immutable identifier that relates to that will be used as the natural key.
9. In either case the IMS is not authoritative for the attribute values, as their source documents are. The authoritative information the IMS generates is the unique identifier for each Digital Identity.
10. **High level assurance re-association.** To maintain the integrity of Digital Identities with High and Very High Assurances a biometric is to be captured at the time of Digital Identity creation. This will protect the level of assurance when the person is re-associated with their identity at some point in the future.

## Digital Identity and Persona

As discussed above Person Entities may have multiple *personas*. Personas can often seem like an Identity; however, they are not. They capture the essence of the functional relationship of the Entity to Defence. To highlight the impact personas, have in relation to Identity the main uses of Identity will be discussed with the impact of Persona.

### Authority

The ability to assert authority is one of the prime reasons Identity is critical to Defence. An Entity can assert authority as their Identity, a Persona or both.

1. Where a business system is concerned with the individual entity (e.g., consent for a surgical procedure) the ability to assert individual authority as an Identity regardless of persona is all that is required. However, where the authority stems from one’s position (which will derive from persona), then the assertion needs to be from the Persona.
2. The application of authority is a business level problem and not a technical one. Business systems should be aware of the need for identity or persona authority assertion and should ask (or if possible, infer) which persona to use as appropriate.
3. For example, where a person with an active public servant persona and reservist persona manages staff in both. A leave approval system could present leave request from both sets of staff. As the system would be aware of the source of the different leave requests, the correct persona could be applied to the approvals without the approver being asked. The appropriate delegations for the persona can also be applied (i.e., one persona may not be able to approve over 14 days leave). This supports the idea that persona is a business concept and not one of identity. The person in the example could be authenticated to the system with the one credential (account) derived from their Digital Identity, not a distinct credential for each persona.
4. The actual authority remains with the identity, the persona supplies the delegation. The concept is: ‘Identity X authorised something, as persona Y.’ This is not a new concept in Defence, with signature blocks being an example of this concept, (refer Figure 3).
5. 

Figure 3: Signature blocks use Identity and Persona

### Access Control

The personas may contribute to access decisions. However, information that a single Entity may have access to does not need to be constrained to only the one *active* persona at any time. At anytime a person should be able to access the sum of the resources they have access to via their various *active* personas.

1. Digital Identity will form the basis of system account creation and permission provisioning by the Access Management System. The Digital Identity Primary Key will be used when the Access Control system provisions accounts across multiple systems. This will allow multiple accounts to be correlated across systems and in most circumstances give the user the experience of a having a single account across these systems.

### Audit

Depending on the nature of the business transaction being audited, either the Digital Identity, Persona, or both may need to be logged for the Entity; this is a solution specific decision.

1. Behaviour is a mechanism to identify and protect against the ‘insider threat’ security problem. The ability to correlate activity across systems using Digital Identity simplifies enterprise-wide behavioural analysis; therefore, improving Defence’s security posture.

## Principles

From the discussion the following principles are derived from this reference architecture:

1. Digital Identity is used for authority, access, and audit.
2. Persona is a business concept.
3. Digital Identity ends with the Entity it represents.

## Conclusion

The correct application of the entity types and principles introduced in this reference architecture will help ensure a consistent approach to Enterprise management and security of information. It will help in the consistency of solution development and support a better end user experience.

1. The creation of trusted Digital Identities is the first step in providing Defence with a single understanding of an Entity’s role and therefore access rights to Defence resources. This leads to the end user being able to use a single identity (in the form of an account) across Defence, simplifying their experience while maintaining a secure security posture.
2. However, Identity Management does not solve the problem by itself. Defence must implement Authorisation Management to leverage the Digital Identity.

1. [↑](#footnote-ref-2)