Document:

Reference Architecture

Part:

Authentication Reference Architecture

Dated:

March 2022

Company contact:

Chief Technology Officer

cto@downerdefence.com.au

Contents

1 AUTHENTICATION Reference Architecture iii

1.2 Introduction iii

1.3 Authentication iii

1.4 Principles v

1.5 Reference Models v

1.6 Decision Framework v

1.7 Patterns v

2 to Template Dated 31 Mar 2022 vi

3 An example annex vi

4 An example appendix vi

Figures

[Figure 1: Federation iv](#_Toc99640326)

[Figure 2: Identity Schema iv](#_Toc99640327)

Tables

**No table of figures entries found.**

# AUTHENTICATION Reference Architecture

### References:

## Introduction

Across our business, there is an increasing level of technical interoperability required to enable nations to conduct missions. Trust between enterprises is an essential part of life, human interaction depends on it.

1. Nations that share partnerships naturally cannot verify foreign personnel, however, trusts that the foreign government does. Maintaining an elevated level of trust with parties enables acceptance of various management standards, practices, and policies, such as determination of identity, local authentication mechanisms, privileges, and non-reputability of identifiers.

### Definition

*Authentication* verifies who you are. It is used to inform Access Control that enables the right entities to access the right resources at the right times, for the right reasons and in what ways.

1. The function for establishing the validity and assurance of a claimed identity of an entity in an information or communications system, by testing the credentials supplied by the entity making the claim/assertion.

### Scope

*Authentication* is relevant to multiple fields that cover both the logical aspects of technology and non-technology areas (for example physical assets).

1. This Reference Architecture is only concerned with the technology areas that pertain to Authentication within the *Defence Information Environment*.

### Audience

This document is for solution architects and capability planners. It is intended to guide and constrain technical solutions to fit within the overall our enterprise. Planners involved in the capability planning function should apply the language and concepts introduced to ensure a consistent approach.

## Authentication

Authentication is used to determine whether someone or something is, in fact who or what it is declared to be. Authentication may contribute towards access control; however, it is not the same.

1. Authentication can be:
2. **Direct.** Interaction occurs inside the application boundary, without the need for an intermediary. If the shared secret between a requester and application is compromised, only the relationship between those two parties is compromised and not the entire model.
3. **Brokered.** Interaction occurs outside the boundary of the application, where an intermediary acts on behalf of an entity. An intermediary manages trust centrally, which eliminates the need for each entity and application to independently manage their own trust relationships. Examples of brokered authentication include Public Key Infrastructure, Kerberos, SAML, and OAuth.

### Federation

Most modern applications have the potential to simplify authentication logic; these types do not provide mechanisms for managing the identity lifecycle of an entity. Figure 1 shows that shifting the authentication layer outside the traditional model means that the application does not hold onto sensitive data, therefore implies federation.

Figure 1: Federation

Figure 1: Federation

1. In technology, Federation implies linking a person’s electronic representation of an identity and attributes stored across multiple distinct systems. This provides collaboration capabilities across multiple applications that may be distributed across organisations, geographies, or business units.
2. Partners that interact with Defence may be subjected to further shifting of their token’s claims. This is due to the nature of the defined set of schemas which may contain existing attributes into the identity schema of an application. Other applications may contain variations of identity schemas which may introduce new attributes that are not specified. Therefore, the identity aggregation needs to know the attributes that are semantically equivalent to one another. Figure 2 represents the interaction of several autonomous units, with a greater need for interoperability.

Figure 1: Federation

Figure 2: Identity Schema

Authentication techniques are used to validate an entity’s identity using identifiers based on various techniques, ranging from simple logon something the entity knows, to more complex mechanisms based on what the entity is, such as retinal pattern, hair colour or other biometric identifiers.

### Trust

Skipping trust before authentication occurs introduces the risk of an agent acting under false identity. Technology enables capability which identifies identity mismatch patterns by scanning the agent before authentication occurs.

1. Trust is one of the key elements in federation. Trust may vary; however, fundamentally it contains authentication between organisations that have established trust for shared access to a set of functions. Using Reference D, trust is determined by:
2. **Level 1.** Little or no confidence in the asserted identity’s validity.
3. **Level 2.** Some confidence in the asserted identity’s validity.
4. **Level 3.** High confidence in the asserted identity’s validity.
5. **Level 4.** Extremely high in the asserted identity’s validity.
6. Authentication consists of various parts. Fundamentally, we care about:
7. **Agent.** Using Reference C, non-person entity, such as network-aware object, usually part of the Defence Information Environment. Facilitates interaction directly to the functionality of an application.
8. **Function.** Using Reference E: ‘A relation or expression involving one or more variables. From an authentication point of view, we are talking about applications.
9. **Identity Store.** Repository that contains electronic representations of person and non-person entities.
10. …
11. Deployed nodes and levels of trust.

### Log On

To verify an identity of an entity, various techniques known as personal identifiers may be used to confirm that identity. These include:

1. **Knowledge factors.** Something the person knows, such as password, pass phrase, personal identification number or challenge response.
2. **Ownership factors.** Something the person has, such as identification card or security token.
3. **Inherence factors.** Something the person is or does, such as fingerprint, retinal pattern, DNA sequence, facial or voice recognition.
4. Entities are issued with credentials which are typically held by a third, trusted party, such as an authority. This provides establishment of the identity of an entity which may provide interaction, thus granting access to an application described as log on.
5. Credentials are usually supplied as documentation, and may contain a key, personal identification number (PIN) or a phrase, are also commonly referred to as passwords. Credentials may be based entirely on knowledge techniques or may be used in combination with ownership or inherence techniques to avoid another entity from assuming that identity.

## Principles

The following principles are introduced to support this reference architecture:

1. *Authentication* must inform Access Control, therefore must operate within a contiguous unity.
2. Identity shall be invisible to the end user; identity, attribute verification and exchange should be a background operation until such time that increased levels of user verification is required.

## Reference Models

From the discussion above it is evident that…

## Decision Framework

This section introduces the ‘so what.’ Now that we have introduced concepts, terminology, and any relationships, how do we apply the patterns and standards?

1. …

## Patterns

The following questions need to be answered:

1. How do services get discovered…
2. …
3. The following

### Annex:

An example annex

### Enclosure:

There is not an enclosure

# to Template Dated 31 Mar 2022

# An example annex

This is an example Annex.

### Appendix:

An example appendix # to Annex A TO Template Dated 31 Mar 2022

# An example appendix

This is an example annex.