ICT Project Guidance

Integrations: Identity Providers for Authentication

Author:

Sky Sigal, Solution Architect

## Description

This document describes the reason, considerations, and methods to use to integrate with Identity Provider (IdP) services.

## Synopsis

The recommended approach for authentication of end users is to use Identity Providers (IdP) that uses OIDC to authenticate end Users, and OAuth to authenticate of 3rd party systems consuming the service’s Application Programming Interface (API) endpoints.

## Contents

[Description 1](#_Toc146892365)

[Synopsis 1](#_Toc146892366)

[Contents 2](#_Toc146892367)

[Introduction 3](#_Toc146892368)

[Objective 3](#_Toc146892369)

[Risks 3](#_Toc146892370)

[Options 4](#_Toc146892371)

[Resolution 4](#_Toc146892372)

[Heading Level 3 4](#_Toc146892373)

[Heading Level 4 4](#_Toc146892374)

[Appendices 5](#_Toc146892375)

[Appendix A - Document Information 5](#_Toc146892376)

[Images 5](#_Toc146892377)

[Tables 5](#_Toc146892378)

[References 5](#_Toc146892379)

[Review Distribution 5](#_Toc146892380)

[Audience 5](#_Toc146892381)

[Structure 5](#_Toc146892382)

[Diagrams 5](#_Toc146892383)

[Terms 5](#_Toc146892384)

## Introduction

People that start a session on a system as unauthenticated public users can convert the session to an authenticated one by providing credentials (usually an identifier/username and password) known only to the user and the system that verifies them.

While two decades ago it was still common practice to persist user credentials in the system, it has long been a top recommendation of the Open Worldwide Application Security Project (OWASP) avoid persisting credentials in a system, and favour using standard protocols to communicate to a 3rd party service dedicated to securing credentials.

## Risk

Beyond technical risks common to all services and devices there is a risk that arises from poor design to use an Identity Provider for tasks beyond identity provision. Namely for implementing centralised Access Management.

This is the market that IAM solutions address.

Such a design has the appeal of reusing a common service that dependent systems are already connecting to pass messages – in this case the name of a role - to them.

However, IAM solutions that reuse identity tokens for authentication needs present a number of design issues:

* It is misusing a service to perform a different service than it was designed for[[1]](#footnote-2).
* Beyond implementing an agreed convention, the sending of a role name in the returned token message does not provide any guarantee that the dependent service will read the message or implement a decision according to it.
* Role based management is a relatively simple and coarse-grained[[2]](#footnote-3) approach to authorisation. It’s inability to be modified on a case-by-case basis, means the larger the number of systems and users the IdP has to service, the more certainty that the Role definition will not meet everyone’s and every serviced context’s expectations.
* The dependent system is not exempt from requiring customisation to perform the non-standard pattern of extracting role titles from the returned token message.

Resolution

A more resilient design does not confuse or combine Identity Management (IM) capabilities with Authorisation Management (AM) capabilities.

While the dependent service uses an Identity Provider (IdP) to provide identity management, it *also* uses a separate Authorisation Management (AM) service (preferably an Authorisation-as-a-Service) to provide advisement on authorisation choices.

For this reason, this paper only concentrates on a dependent service’s reliance on an Identity Provider.

Components

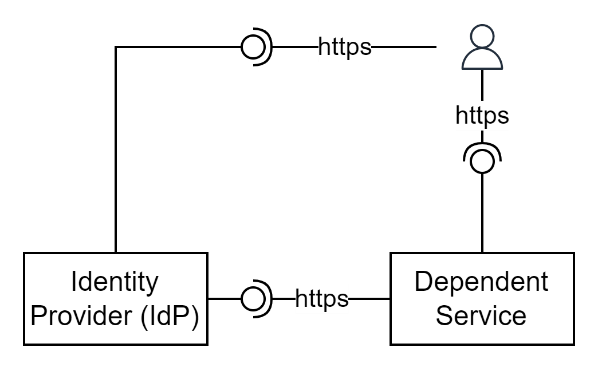


Figure : Service Devices

Information

Messages between the two services flows through the service consumer’s service agent (their browser).

Messages

The type of messages sent back and forth are

Flows

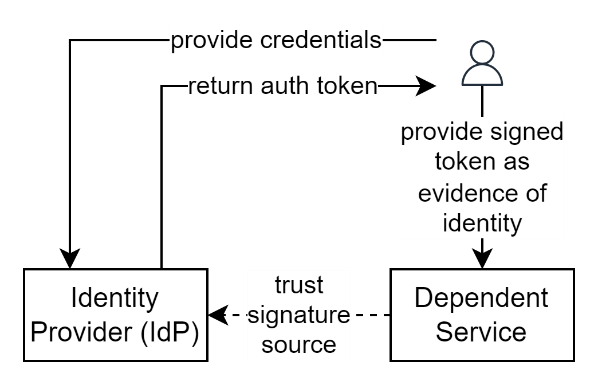


Figure : IdP Information Flows (HL)

Appendices

Appendix A - Document Information

### Images

[Figure 1: TODO Image 2](#_Toc144995112)

### Tables

[Table 1: TODO Table 3](#_Toc145048484)

[Table 2: TODO Table 2 3](#_Toc145048485)

### References

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
|  |  |
|  |  |
|  |  |

### Audience

The document is technical in nature, but expected to be accessible for validation and/or use by a non-technical audience.

### Structure

Where possible, the document structure is guided by either ISO-\* standards or best practice.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (ArchiMate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.

### Terms

Refer to the project’s Glossary.

##### Term

: the meaning.

1. It is defined as an authentication *Identity* Provider – not an *Authorisation* Management Service. [↑](#footnote-ref-2)
2. As opposed to a more fine-grain authorisation mechanism [↑](#footnote-ref-3)